Migration Letters

Volume: 21, No: S5 (2024), pp. 721-738

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

A Clone Detection Mechanism For Hybrid Wireless Sensor Networks (Hwsns)

Swetha P M[1]*, Dr. Prasanna B T[2]

DOI:10.47059/ml.v20i4.xyz

Abstract:
Hybrid Wireless Sensor Networks (HWSNs) encompass an assembly of both fixed and mobile beam joints endowed with limited sources, functioning typically in adverse settings such as battlefields and reconnaissance regions. Due to their inherent characteristics, HWSNs often operate unattended and lack tamper-resistant tools. An adversary can effortlessly seize nodes, analyze and duplicate them, clandestinely placing these replicas strategically within the network. This paper focalizes on the node replication attack in HWSNs, acknowledging its significance. It delves into the existing advanced-of-the-art regarding joint repetition attacks, providing an exhaustive overview of prevailing recognition and restraint machines from the information. The intention is to foster a deeper comprehension of factors crucial for designing effective defense mechanisms against cloning attacks. Given the unattended description and absence of tamper-resilient ironware, device systems are vulnerable to various attacks like Sybil, Eavesdropping, and Denial of Service. Among these, the node clone violence stands out as a menacing threat, involving the capture of a node, extraction of its confidential information, replication, and insertion of these duplicates into the network for malicious purposes. This paper introduces a novel clone detection algorithm tailored for identifying clone attacks in hybrid wireless networks. The algorithm proves instrumental in mitigating communication costs, reducing routing overhead, and enhancing overall network throughput.

Keywords: *Wireless Sensor Networks, Clone Detection, Static and Mobile Wireless Sensor Nodes, Clone nodes.*

1. Introduction.

A Wireless Sensor Network (WSN) encompasses diminutive sensors equipped with modest processors, limited memory, wireless modems, and constrained battery or power sources. Recent strides in tiny embedded systems have elevated WSN as a pivotal technology in diverse applications, including security, environmental observing, medical equipment, food preservation, agriculture, energy management, inventory control, water gauging, industrial processes, and building automation [1].

In the perspective of a structured Wireless Sensor Network (WSN), there is typically a meticulously designed architecture and well-defined network management. On the contrary, an unstructured WSN often comprises a multitude of sensor nodes with a less transparent network management. In unstructured WSN scenarios, sensor nodes are frequently deployed in an ad hoc fashion without a centralized infrastructure. Following deployment, these sensors operate autonomously without continuous oversight.

Security remains a formidable challenge within Wireless Sensor Networks (WSN) [2, 3]. Numerous research endeavors have been undertaken over the years to tackle security concerns in WSNs. Defeating [4, 5], node localization [6, 7], time harmonization [6], and information accumulation [7, 8] are among the common purposes in WSNs that are

[1]*Assistant Professor, Department of Computer Science and Engineering, JSS Science and Technology University, Mysuru-570006

[2]Associate Professor, Department of Computer Science and Engineering, JSS Science and Technology University, Mysuru-570006

susceptible to defense breaches. Researchers have identified various novel attack vectors pursuing WSNs [9], including Sybil and wormhole attacks [10], basic layer occurrences [11], sinkhole and Hi overflowing attacks [12], and duplicate attacks.

With the progress in automation and microchip tools, a device node can now incorporate mobility functions. The implications of mobility on Wireless Sensor Networks (WSNs), especially concerning network security, pose notable challenges. In unstructured WSNs with a substantial animated of mobile sensor nodes, safeguarding the group necessitates more intricate measures to ensure organized connectivity and detect failures. It is worth noting that techniques devised for securing static WSNs may not seamlessly apply to the implementation in Hybrid WSNs (HWSNs).

In a general context, a duplicate occurrence is recognized as an bid-autonomous defence intimidation [8], wherein sensor nodes fall under the complete control of attackers within the network, appearing as initial and authentic bulges. In a duplicate incident scenario, an adversary, typically a human, seizes an initial intersection from the interact or approach. By utilizing stealthy authorisation such as instructions, identity information, and cryptographic resources, the attacker reproduces clone nodes and reintroduces them into the network [3]. Consequently, the attacker gains the capability to oversee the entire network communication, manipulate the Wireless Sensor Network (WSN), inject false information, disrupt signals, alter cluster formations, manage various protocols, disable WSN functions, and perform other malicious actions [13].

Furthermore, in Hybrid Wireless Sensor Networks (HWSNs), the honest environment of the environment and the mobility of points contribute to the intricate challenge of detecting clones. Distinguishing between legitimate and illegitimate nodes becomes notably more difficult. As outlined by Parno et al. [14], an adversary has the capability to Assistant Professor Department of Computer Science and Engineering JSS Science and Technology University, Mysuru-570006

generate numerous replicas swiftly. The utilization of readily available tools facilitates the compromise of nodes within a relatively short timeframe.

As previously mentioned, the inclusion of node mobility in Hybrid Wireless Sensor Networks (HWSN) adds a layer of complexity beyond that of static WSNs. Consequently, the detection of node repetition or clone hits in HWSN proves to be more challenging compared to traditional WSNs. Zhu et al. [3] have conducted a comprehensive review of security threats posed by clone attacks and have explored existing detection procedures, evaluating their strengths and weaknesses in both static and mobile WSNs. This examination serves as inspiration for our paper, guiding its structure to provide readers with extensive guidance and recommendations on existing methods for detecting replicas in the HWSN environment. Consequently, this paper aims to furnish researchers, inventors, and developers with comprehensive insights, understanding, and support concerning clone detection methods in HWSNs.

(1) The assailant possesses intelligence, proactiveness, and effective command attributes, enabling the establishment of a imitation of a active joint [15]. Moreover, it retains the ability to covertly seize authentic device nodes [14].

(2) The attacker can produce duplicates or replicas of bumps using cryptologic substance acquired from the imprisoned node. Additionally, the attacker retains the ability to monitor and exert control over both the captured node and the duplicate joints at any given moment.

(3) The primary aim of the aggressor is to shield its duplicates from detection, as the discovery of any clone may necessitate the initiation of a revocation procedure for all clones. Once a mobile Wireless Sensor Network (WSN) detects a clone, it may institute a examining procedure to identify other duplicates in the complex [16].

(4) The invader holds significant influence and can pose threats to bumps that might function as observer bumps. Consequently, it can be inferred that interfere-unaffected active points in Hybrid Wireless Sensor Networks (HWSN) may struggle to withstand a sophisticated attacker. Furthermore, the clones possess mobility, adding an extra layer of complexity to the detection process.

1.1 Clone Attacks in Static and Mobile WSN.

1.1.1. Clone Attacks in Static WSN. The duplication of entities can transpire swiftly, and the same applies to clone attacks within Wireless Sensor Networks (WSN). Figure 1 elucidates the commencement and creation of cloning attacks within a WSN. Given the unattended nature of WSNs and their inability to incorporate tamper-resistant hardware, malevolent actors can effortlessly capture nodes. Upon obtaining crucial information such as identity, secret keys, codes, or cryptologic substantial, the assailant can reprogram the bulge and reintegrate these duplicated nodes into the network. Exploiting the unattended behavior of WSNs, adversaries can readily manipulate the nodes. Following the acquisition of knowledge and the reprogramming of the node, the attacker can transmit it back into the network. With just a single node, the attacker possesses the capability to generate multiple replicas of the same node.

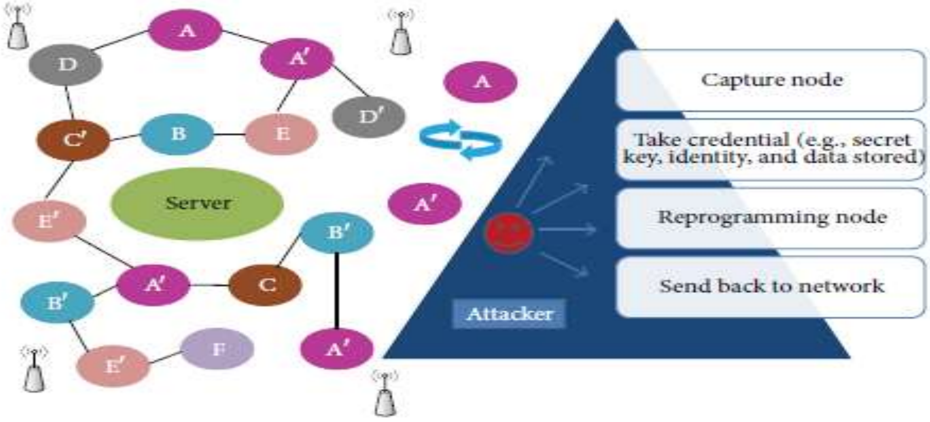


Figure 1: Clone Attack Scenario in WSNs

Figure 1 illustrates A as the original node, and A' represents numerous replicas of A. Consequently, distinguishing between the original node and its replicas becomes a formidable task. Sensor nodes within a WSN are organized, confirmed, and distinguished by specific identities (IDs). In the interact, the replicates precisely mirror the authentic mobile node that was captured. Therefore, the entire set of attributes, including the characteristics (ID), needs to be duplicated. If the undisclosed and secure attributes are duplicated but the active joint ID is omitted, engaging in mischievous happenings within the Mobile Wireless Sensor Network (MWSN) becomes an implausible endeavor.
The primary focus revolves around a crucial methodology for Mobile Wireless Sensor Networks (MWSN), wherein keys are pre-allocated to a mobile node through itself before deployment. This ensures that the entire cryptologic functions are tied to the ID [3]. It is imperative for a sensor node to sufficiently validate the to others, and sign-based uniqueness has become integral for clone alleviation in Wireless Sensor Networks (WSN), including the ID-based sign method [14]. Extensive and comprehensive discussions regarding sign-based schemes have been documented [14]. Ongoing advancements in sign-based methods have yielded honest achievements and practical implementations [21]. Conversely, the constrained power supply and limited retention pose significant constraints on the volume of authentication and justification knowledge that can be stored, updated, and replaced within the system. Accordingly, the primary execution conditions for joint duplicate recognition, as determined by the current study analysis, prioritize problem resolution, specifically aiming to minimize energy consumption and memory usage [22].

1.1.2 Clone Attacks in MWSN.

A distinct subset within Wireless Sensor Network (WSN) functionality plays a crucial role in executing various operations, recognized as Mobile Wireless Sensor Networks [23]. In contemporary research, WSN movement has evolved into a pivotal and prominent area of exploration. Initially, transportability was confronted with several challenges such as connectivity, coverage, and energy consumption, despite the fact that WSN deployments were not initially conceptualized as entirely stationary. However, recent studies embrace mobility with optimism and understanding, contrary to the earlier perspective [24]. Instead of complicating replica detection tasks, it is now recognized that the integration of mobile applications can effectively address major issues related to replication detection [25]. Moreover, mobility empowers sensor nodes to track various phenomena, including chemical clouds [26]. A critical consideration for Mobile Wireless Sensor Networks (MWSN) is the essential requirement for localization. Mobile nodes can maintain a secure distance from fire boundaries, providing real-time information and updates to firefighters about the location of the boundary at any given time.

A Mobile Wireless Sensor Network (MWSN) is designed for wildfire observation, allowing mobile sensors to track and adapt their paths as the fire spreads. The mobility aspect facilitates the creation of multiple communication pathways, ensuring data integrity, increasing conduct competence, and minimizing the amount to of steps required for missive transmission [27]. The device points, distributed across the atmospheric points, form a multi-hop mesh system. A mobile node performs as an developed sensor node, encompassing all the functionalities of a stationary sensor node while introducing the convenience and adaptability of mobility. The base station functions to bridge connections to additional system, such as the Internet [28].

Figure 2 illustrates the process of generating reproductions in the MWSN, depicting how attackers compromise mobile nodes and reintroduce them into the association for mischievous actions. Figure 2(a) depicts the disposition of moveable bulges in MWSN, Figure 2(b) illustrates the concession of a movable bulge by an attacker, and subsequent alteration of information sent back into the network for spiteful actions, while Figure 2(c) displays the presence of both unique and replicated mobile nodes with identical geographies in MWSN. The red color signifies the existence of replicas, considering that in MWSNs, the replicated nodes possess mobility. Consequently, distinguishing replicas from initial nodes in MWSN becomes highly challenging due to the movement appears.

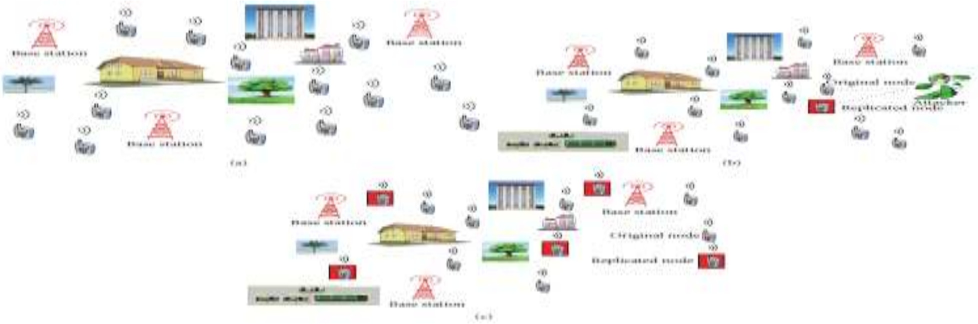


Figure 2: (a) Mobile nodes adopt in MWSN. (b) Attacker negotiate the mobile node and after modifying the communication send again back into system for mischievous activities. (c) Original and duplications mobile points with same features in MWSN.

1.1.3. WSN and MWSN Comparison. When delving into Mobile Wireless Sensor Networks (MWSN), it becomes crucial to examine the significant distinctions between still WSN and MWSN across various aspects such as localization, active network analysis situs, power ingesting, and system sink [23]. Table 1 outlines several key variations involving fixed and mobile WSNs concerning replication attacks. In scenarios involving lightweight or displaced systems, or formerly inactive nodes, inactive active sensors can strategically join or fill the voids in consultation and supervising paths. This capability is unattainable in static WSNs, as data from inactive, severed, or isolated points would simply vanish. Similarly, when stationary drops are employed, sensor nodes closer to the base station experience faster depletion. Hence, they must transmit communication data more promptly than nodes situated farther away. This challenge can be effectively addressed by incorporating mobile base stations, thereby enhancing the network's lifespan [29]. The primary advantages of MWSN over WSN include broader coverage, enhanced tracking capabilities, increased channel capacity, and superior energy efficiency.

1.2. Literature Review

Numerous approaches have been put forth to identify duplicate occurrences in Mobile Wireless Sensor Networks (MWSN). Figure 3 visually represents the current duplicate recognition methods in MWSN. Broadly, these recognition structures can be classified into two main groups: unified and allocated. The subsequent subsections will delve into a detailed discussion of these two methods.

1.2.1. Centralized Method. In the context of centralized detection for mobile node replication attacks, all nodes transmit their information to a singular location, such as the centre station, for decision-making and information aggregation. For instance, if two mobile sensor nodes share identical identities but are located differently in the system, the base station can readily discern the replicated node. However, this strategy has a notable weakness—a single point of failure. The reliance on one point for checking all replica nodes renders the entire network susceptible to control by the attacker if the replication goes undetected (due to the single point of failure). Another drawback is the sluggish nature of this method, as each node must await its turn, potentially causing congestion and network delays. The subsequent section outlines research findings related to centralized detection methods.

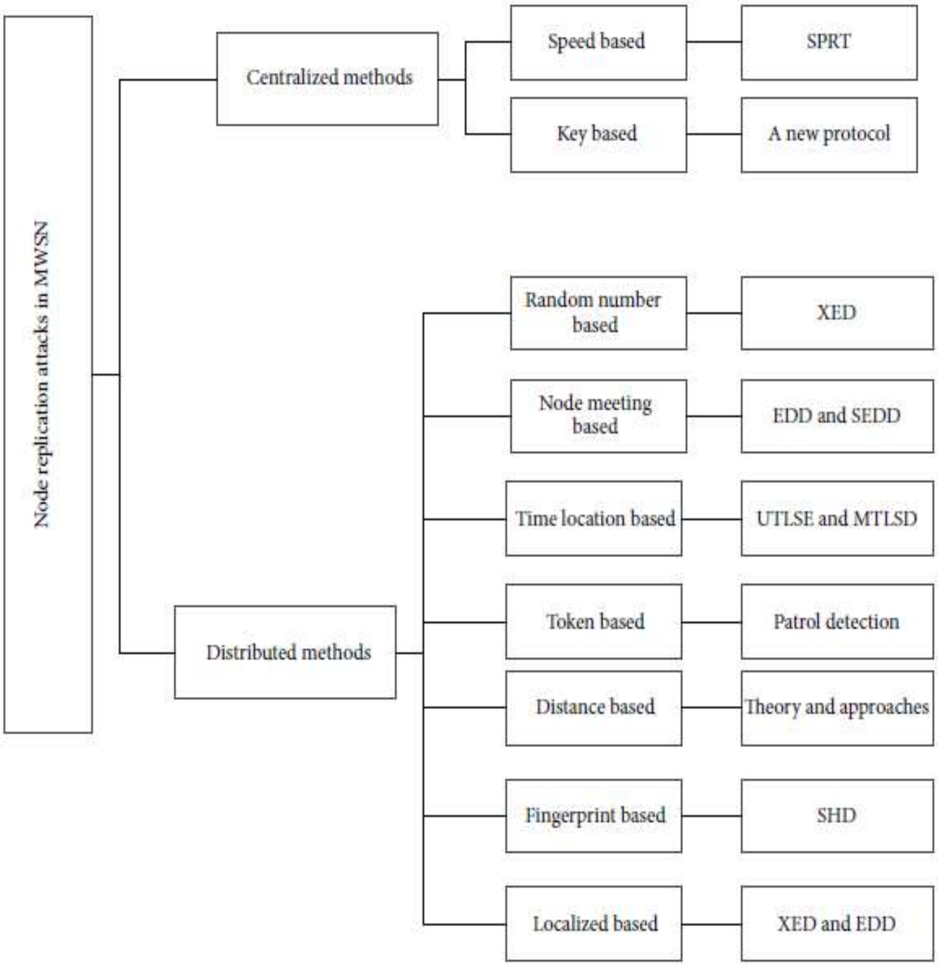


Figure 3: Overview of work done in detection of cloning attacks in MWSNS.

(1) Swift Detection of Mobile Node Replication Attack with Speed-Based (SPRT). Ho et al. [30, 31] introduced a rapid recognition technique for mobile node duplication attacks

aimed at identifying replicas. This method involves assessing and evaluating the pace of the connection at a consolidated point using the SPRT. The approach is grounded in a chance move, where the null hypothesis (indicating a non-clone node) sets the minimal confines, and the alternate proposition sets the upper restrictions with each thought. The establish location processes the speed of the nearby asserts, as the rapidity of a replicated cell device intersection would not surpass the network's estimated speed.

Additionally, the authors outline the communication design containing the indicator and the aggressor as a frequent game, determining the Nash equilibrium [30, 31]. The authors conduct imitations created on a undertaking occurrence approach, where the opponent assumes that duplicates transfer inadvertently within the network, and under a static position attack scenario, where the adversary prevents his duplicates from affecting to elude recognition. The outcomes of these simulations demonstrate that the proposed technique swiftly reveals connection duplicate incidents in Wireless Sensor Networks (WSN) with movement.

1.2.2. Distributed Method. In the context of mobile node duplication attacks, allocated uncovering deviates from the reliance on a centralized point, such as a base station. Essentially, this approach involves the random selection of a witness node responsible for claiming the communication or locality, contingent on the scenario, for the detection of node replica attacks.

The following is a study on distributed method.

(1) Robust Detection of Node Replication Attacks (XED) in MWSN:

In their work, Yu et al. [33] introduced the Resilient against Node Replication Attacks protocol, known as XED (Extremely Efficient Detection), employing the memorize and dispute method to identify duplication nodes in MWSNs. The protocol focuses on the scenario when two nodes are in communication range. During this encounter, they engage in generating and exchanging random numbers, concurrently storing node IDs in memory using a table. If, during the random number exchange, a node fails to respond correctly or replies with an incorrect random number, efficient detection of a replica is achieved. Upon subsequent encounters between the same nodes, the initially saved random number is replaced with a new one. Importantly, this strategy de-emphasizes the need for location information. The distinctive feature of XED lies in its ability to sharply detect clones at each move. The protocol dictates that when one cell intersection advances another, they exchange accidental integers to confirm there is no earlier interaction. Instead, unintentional number exchange occurs at available times when the cell joint requests the numbers from others. If a mobile node fails to respond or provides an incorrect value not matching the one in recollection, it unequivocally affirms the identification of a clone. Notably, when a clone encounters legitimate nodes, it may mistakenly assume prior interactions. Conversely, clones are also revealed if recognized nodes possess proof proving no prior meetings.

(2) The notable features of EDD and SEDD include:

1. Distributed Detection: EDD and SEDD employ a distributed approach, eliminating the need for a centralized base station. The protocols are orchestrated through mobile node clones, enhancing resilience and adaptability.
2. Individual Detection: Each mobile node operating within the EDD and SEDD framework possesses the capability to autonomously distinguish clones. This individualized detection mechanism contributes to the overall robustness of the protocols.
3. Network-Wide Revocation Avoidance: The reversal of clones is a network-wide endeavor, achieved through every mobile node. The protocols facilitate this process by systematically broadcasting revocation communications across the entire system.
4. Efficiency and Effectiveness: EDD and SEDD exhibit commendable efficiency in recognizing clones, ensuring a higher level of recognition efficiency. This efficacy is achieved with communication overheads of (n) in worst-case scenarios and (1) in average scenarios.

Additionally, the EDD strategy relies on assessing the total encounters a node has with a specific node within a limited time period. For effective detection, the cloned node must encounter the same identity more times than a predefined threshold (length T) in the network. When a node exhibits disparate behavior, it raises suspicion of potential replication or cloning. This technique operates through offline and online steps. The offline step calculates the time interval (T) and the threshold (ψ) before deployment. The online step involves threshold comparison within a specific time interval (T) against the number of chance meeting.

Moreover, the SEDD (Storage Efficient Distributed Detection) strategy optimizes storage overhead by monitoring a split of lumps known as the display set, as opposed to monitoring all nodes in the network. This reduction in storage requirements enhances the overall efficiency of clone detection.

UTLSE Protocol:

- Information exchange among witnesses occurs when they encounter one another, facilitating clone detection.
- When two or more nodes encounter each other, they interchange their time-place claims. If a observer intersection is not within the statement range, it withholds the claim until a subsequent encounter.

MTLSD Protocol:

- Both UTLSE and MTLSD operate as encounter-based systems, generating and dispatching messages exclusively when two or more nodes meet. This strategy ensures that no routing signaling messages are required for the detection process.
- MTLSD focuses on optimizing the performance of replica node detection by enabling witnesses to manage multiple time locality applications for studied mobile sensor joins.

(4) Patrol Detection of Replica Attacks in MWSN:

Wang and Shi [36] proposed a guard revealing method for identifying node replication attacks in Wireless Sensor Networks (WSN). This method incorporates both stationary and mobile modes for detection. Mobile sensor nodes serve as patrollers distributed across various zones within the sensor network to identify cloned sensor nodes.

Detection Methods:

- Two types of detection methods are employed: inactive and mobile modes.
- Mobile sensor nodes are designated as patrollers and distributed across different regions to identify clones.

Identification Criteria:

- Nodes with identical identities (ID) among distinct areas are considered clones or compromised nodes.
- Detection also involves verifying if a mobile sensor node is traveling at a speed higher than the designated maximum speed.

Operation:

- Mobile sensor nodes, acting as patrollers, send declared messages to devices in the network.
- The network is initialized with the assumption of no attacks in the early stage.
- Every sensor node is patrolled by at least two mobile nodes, and the static node retains the

Detection Process:

- Each round is divided into different levels, and patrollers shift towards zones to broadcast claim messages.
- Patrollers analyze the position and distance of sensor nodes after receiving claims.
- Lists of messages are generated in white-list (original nodes' claims) and blacklist (replica nodes' claims).

- Replica identity is revoked by denying confidential sources.
- If duplicates are positioned in a area where a patroller groups their message replies, and the distance is higher between locations, the patroller can promptly reverse them.
- If clone replies are acquired by various patrollers, they will be managed through message interchange or reported to the base station.

Considerations:

- Original mobile patrollers wait for replies after reaching new locations and sending claims at specified time intervals.
- Detection depends on multiple steps, including speed checks, patrol claims, storing data in white and black lists, and distance-based comparisons.

(5) Single Hop Detection of Node Clone Attacks (SHD) in MWSN:

Lou et al. [37] proposed the Single Hop Detection (SHD) for identifying node duplication attacks in Mobile Wireless Sensor Networks (MWSNs). The key features of this method include the acknowledgment of movement as an advantageous factor in clone detection, contrary to the perception of node mobility as a disadvantage in many proposed solutions for static wireless sensor networks, predominantly relying on location-based witness detection schemes. This flexibility is crucial for the adaptability of SHD to the dynamic nature of MWSNs.

In SHD, the mobility of nodes is not viewed negatively; instead, it is leveraged to enhance clone detection. Unlike traditional approaches, which may not be suitable for MWSNs due to the mobility factor, SHD remains effective even when replicate nodes can instantly contact each other. The practice demonstrates particular strength against clones colluding attacks, providing a robust defense mechanism.

In the first scenario, involving a fingerprint claim, each node generates a signed list of neighboring nodes. This signed list is integral to the SHD operation and relies on physical proximity within the node's local neighborhood community. Notably, the single hop neighbor node list is essential for Wireless Sensor Network (WSN) communication, emphasizing the significance of nodes being aware of their neighbors for effective communication.

The SHD protocol's efficacy is rooted in its reliance on single hop neighbors, which prove to be highly robust. The protocol successfully detects imitation attacks through two essential situations: the initial privilege for impressions and the subsequent proof of impressions, showcasing its resilience and effectiveness in securing MWSNs against node replication threats.

(6) Localized Algorithms for Detection of Node Replication Attacks in Mobile Sensor Networks: Yu et al. [38] purported two revealing systems, XED (Extremely Efficient Detection), and EDD (Efficient and Distributed Detection), for combating node duplication attacks in Mobile Wireless Sensor Networks (MWSN). This local procedure comprises two distinct methods:

(i) Extremely Efficient Detection (XED):

In XED, the core concept involves the exchange of random numbers between nodes. When nodes meet, they exchange random numbers, storing them for future encounters. XED operates in two steps: an offline step completed before sensor disposition and an online step executed after disposition by each node. XED's effectiveness relies on the assumption that clones cannot collude with other nodes. The method considers that the entire swapped messages should be preserved without specifically noted. The potential issue arises if clone nodes can interconnect, allowing them to share the latest received random numbers. This could undermine detection, as clone nodes might respond with the correct arbitrary number when encountering initial nodes.

(ii) Efficient and Distributed Detection (EDD):

The primary theory following EDD is to observe the extreme number of times a node meetings another node within a fitted time period, regulated with high possibility. EDD recognizes that the least number of eras a node confronts replicas with duplicate identity ought exceed a tolerance during the same time separation. The detection method operates in two phases: an offline phase completed before sensor deployment and an online phase executed by each node at every move.

Both XED and EDD contribute to localized detection techniques, emphasizing efficiency, effectiveness, and network-wide synchronization and revocation avoidance. These algorithms offer robust solutions for countering node replication attacks in MWSNs, ensuring the integrity and security of the sensor network.

1.2.3. Comparison of Existing Approaches

Concerning the detection of replication attacks, existing approaches exhibit limitations that impact their overall efficiency. The initial methods' constraints are underlined below and shortened in Table 2 for convenient relationship. Table 2 provides a summary of all MWSN detection methods, outlining communication cost, and fast detection parameters [15]. Each solution for replica node detection offers a distinctive analysis, motivation, and techniques, with both positive and negative aspects. Consequently, determining the optimal strategy proves challenging. Security emerges as a significant concern in MWSN, and the swift and effective detection of node replication is crucial. Failure to promptly identify replication threats may enable attackers to compromise the entire network, utilizing it for malicious activities.

Detection method	Methods	Communication cost	Memory cost	Fast
SPRT [30], [31]	Speed based	$O(n\sqrt{n})$	$O(n)$	Yes
ANewProtocol [32]	Key based	$O(n \log n)$	—	No
XED [33]	Random number based	$O(1)$	$O(4 \cdot d \cdot E[X])$	No
EDD [34]	Node meeting based	$O(1)$	$O(n)$	No
SEDD [34]	Node meeting based	$O(n)$	$O(\zeta)$	No
UTLSE [35]	Time location based	$O(n)$	$O(\sqrt{n})$	No
MTLSD [35]	Time location based	$O(n)$	$O(\sqrt{n})$	No
Patrol Detection [36]	Distance based	$O(n)$ & $O(n * \sqrt{k})$	—	No
Theory and Approaches [3]	Token based	—	—	No
SHD [37]	Fingerprint based	—	—	No
XED [38]	Localized based	$O(1)$	$O(n)$	
EDD [38]	Localized based	$O(1)$	$O(1)$	No

Table 2

As stated in the preceding segment, consolidated approaches such as SPRT and a new procedure rely on a base station. Central approaches hold the benefit of rapid replica detection, as seen in the SPRT method, which involves a single-point check. However, this centralized dependency poses a potential disadvantage in the event of a single point failure. The swift detection of node replica attacks using sequential analysis (SPRT) has been introduced in [30, 31]. Fundamentally, their strategy is built on the premise that unique mobile nodes should not surpass the system's maximum speed, while replicas, tasked with assuming positions, will move much faster. Consequently, if the speed of mobile nodes exceeds the system's speed, there is a likelihood of two nodes with identical identities coexisting in MWSN. SPRT relies on a sequential hypothesis for speed checks on each mobile node; if it exceeds a certain threshold, it is deemed a replica. There is a probability that a replica can fall within a specific threshold, indicating that the replica is also in motion. Additionally, the implementation of the speed measurement tool is expensive and poses challenges for easy integration into networks.

In [32], the authors present a novel protocol for detecting node replication attacks in MWSN. Their approach is rooted in the concept of Bloom filters and a polynomial-based pairwise key pre-distribution, asserting that a clone cannot exist with a real identifier and the pairwise keys of every node. To address the issue of a single point of failure, a distributed approach has been proposed. The Extremely Efficient Detection (XED) [33] is introduced, and its operational principle revolves around the exchange of random numbers at different locations. Consequently, if a mobile node fails to exchange the correct random number or the numbers do not match, it signals the presence of a replica in the network. XED, while effective, does not qualify as a swift detection method, relying on nodes meeting and replacing arbitrary information. This process introduces delays in the detection procedure, potentially leaving the network vulnerable to an intelligent attacker. As noted in [33], replicas may exist in the network without cooperation or communication with mobile nodes, as they can establish secret channels to engage in mischievous behaviour.

The EDD approach relies on node encounters and utilizes maximum memory for information storage, which may not be practical for real-life scenarios in large-scale networks. On the other hand, SEDD mitigates memory concerns by contemplating the screen set but still requires substantial storage. Additionally, it depends on the timing of encounters between two nodes, making it not a fast exposure method.

The approaches to replica detection, specifically Unary Time Location Storage and Exchange (UTLSE) and Multi-Time Location Storage and Diffusion (MTLSD) as proposed in [35], leverage the exchange of time-location claims when nodes come into announcement choice. However, if the observer node the aforementioned is a model node, it poses a threat to the network, as the observe lump is at random selected in this scheme. Additionally, the time-consuming nature of waiting for nodes to interact and exchange information introduces a potential security threat, as an attacker could exploit the delay in the detection scheme.

Alternative hypothesis and method to duplication recognition involve a nominal-grounded way, as presented in [39]. In this method, compromised nodes do not collaborate, and when portable nodes meet, they exchange tokens stored in their memories. During the detection period, each node inquires about the previously exchanged tokens, with an incorrect response indicating a replicated node. The concept of cooperation with every node is also introduced, where if a mobile node is encountered multiple times, it hints at the presence of a replica. However, this scheme may not be foolproof, as replica nodes can also exchange tokens, creating a protocol that exists in name only. An active and intelligent attacker could exploit this and establish a secret channel for replica nodes.

The Single Hop Detection (SHD) method, as purported for duplication recognition in [37], asserts that at accidental moment intervals, a mobile point cannot exist in unique locality clusters. This methodology relies on identification assert and authentication. When two lumps reunite and exchange lists of witness nodes, the presence of a replica is indicated if there are two fingerprint allegations with identical identities and keys in different locality clusters. The SHD procedure emphasizes the identification prerogative and considers the witness for claiming the node. However, it may encounter issues if the observe lump itself is a replicate node.

Two lump duplication recognition techniques established on identified algorithms, namely XED and EDD, have been detailed in [38]. The benefits of restricted algorithms include presents such as restricted uncovering, competence and efficiency, system-wide organization circumvention, and system-wide withdrawal prevention. This method employs the hypothesis of dispute and reaction, distinguishing it from other existent methods. Moreover, in contrast to current methods for replication attack revealing, it also mitigates storage expenses.

1.2.4. Effect of Different Parameters on Efficient Replication Attacks Detection.

Detection Accuracy. The calculation of the probability of accurately detecting a mobile replica occurs when there are two or more nodes sharing the same identity (ID) in the MWSN. Successful detection of a node replica is termed as true positive, while an incorrectly identified replica in MWSN is referred to as wrong optimistic. Wrong disapproving denotes instances where the copied lump is not identified as a duplication, thereby diminishing the competence and efficiency of duplication recognition methods. The recognition process ought exhibit a great true positive rate, indicating successful detection of clone nodes, and a low false positive rate, ensuring that normal nodes are not falsely accused as clones.

Communication Overhead. The likelihood of resources consumption by cell nodes in transmitting and catching communication is crucial. The message expense for detecting copies ought be both acceptable and sharp.

Memory Overhead. Each mobile node is required to store, check, and compare information for the detection of clone attacks, specifically checking for identical node identities. Therefore, each node needs an efficient memory system to store essential data such as bulge characteristics, bulge note, whereabouts, etc.

Detection Rate (Fast or Slow). The detection rate probability pertains to identifying the threat attack within a confined time frame. The likelihood of detection periods indicates that the proposed method efficiently and effectively identifies replicas promptly. Failing quick detection might offer an opportunity for an assailant to exploit delayed detection and compromise overall communication.

Energy. is also a crucial factor in replica detection, as an attacker requires substantial energy to surveil the entire network. Simultaneously, the energy of the mobile nodes must be efficient for executing the detection and mitigation processes for replication attacks.

2. Material and Methods. STBD Cloning Detection

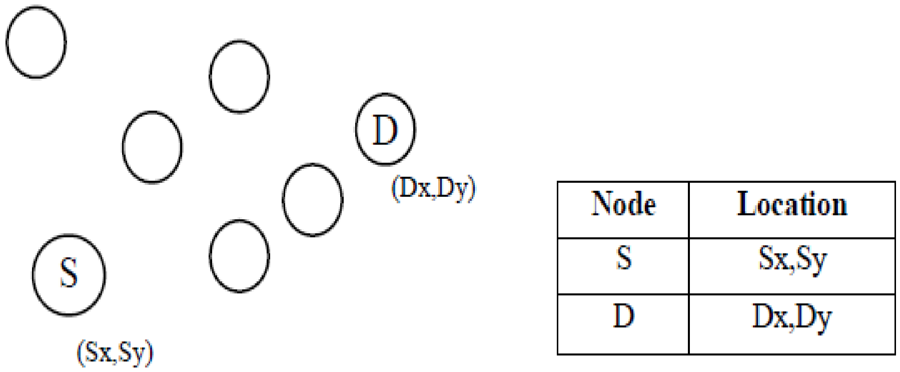
The detection of node clones relies heavily on comprehensive information about all nodes, including neighbor lists, node IDs, and their locations. During the detection process, nodes validate claiming messages, which contain signed reports of neighbor lists, locations, and IDs, and share them with other nodes in the network. These reports are then compared with the recipient's own neighbor list to identify clones effectively [71]. While this approach works well for static networks, issues arise in mobile networks where node locations and neighbor lists are in constant flux, potentially leading to the misidentification of authentic nodes as clones.

To address the challenge of false clone detection and enhance the effectiveness of clone detection, this work introduces the Speed Time Based Detection (STBD) algorithm. The proposed algorithm takes into account the hybrid structure of the network, resulting in significantly reduced communication costs and routing overhead when compared to the existing RDE approach [71]. Furthermore, it contributes to the overall network throughput improvement.

The proposed algorithm achieves more effective node clone attack detection by considering the hybrid network structure. The genuine source node in this work exhibits varying speeds while moving through the network. This dynamic movement generates messages to the destination from different locations at various time intervals, constantly updating its neighbor list. Despite these changes, the destination may mistakenly identify the genuine node as a clone. The proposed work successfully avoids such false detections and ensures accurate node clone attack detection. Additionally, the work enhances the network's transmission capability through multiple stages.

2.1 Network Initialization

Nodes are distributed randomly within the predetermined network area. Each node possesses information about its location and node ID as integral components of its identity, as depicted in Fig. a. In this configuration, every node retains its routing information. It is crucial to note that in the proposed work, the source and destination nodes are unquestionably considered trusted entities.



Node	Location
S	Sx,Sy
D	Dx,Dy

Figure a: Node Deployment

2.2 Optimum Path Detection

Sensor node A creates the claiming message (Mn) intended for neighboring nodes, selected through the implementation of the Greedy Perimeter Forwarding technique [72], which comprises two stages. In the initial stage, nodes determine the closest routers (nodes) based on their own locations, aiming to facilitate the transmission of information to the destination, as illustrated in Fig. b.

In the scenario where Node A aims to transmit information to Node D, Node A examines its table to identify the neighbor with the location closest to Node D within its radio range. In this case, rt_1 emerges as the nearest neighbor to Node A from Node D. The transmission of information occurs from Node A to rt_1, and by employing the greedy forwarding principle, the optimal path A□rt_1□rt_3□rt_4□D is established. Moving to the second stage, the Perimeter Forwarding technique is implemented using the right-hand rule when the neighboring nodes from the first stage are situated farthest from the destination.

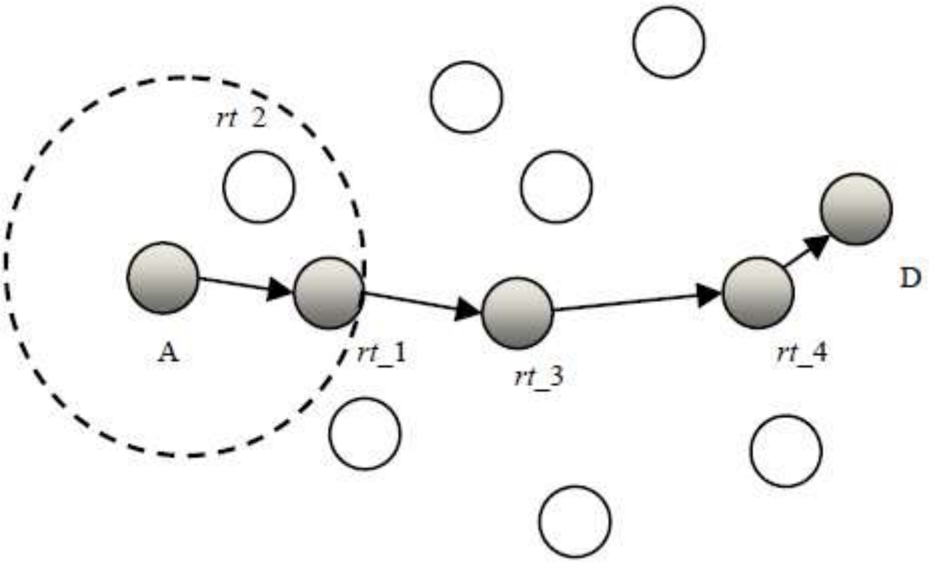


Figure b: Optimum Path Detection

Notably, this approach does not require any cross heuristic to determine the perimeters of the graph. The combination of both stages results in the identification of an optimal path through which the claiming message (Mn) is sequentially passed from node to destination.

$$Mn = (Nid \,||\, Ln(x,y) \,||\, NLn) \qquad (1)$$

Where, Nid = Node ID

Mn = Claiming Message

Ln(x,y) = Location of node
NLn = Neighbor list of node

2.3 Location claim forwarding and Clone Detection

In the presented research, the mobile genuine source node Ng consistently alters its location. The claiming message Mn, originating from the genuine node Ng, reaches the destination at time T, having traveled from the location (xi, yi) through intermediate nodes identified using optimum path detection. Upon receiving another message at the destination from a distinct location (xj, yj) at time Ti, the Euclidean distance between these two locations, (xi, yi) and (xj, yj), is calculated. If this distance surpasses the maximum possible distance (Max_dist) as depicted in (2), the presence of a clone is identified. It is crucial to note that the change in the node's neighbor list due to its mobility is not indicative of a cloning attack. Following the detection of a clone node, the destination terminates the Speed Time Based Detection (STBD), revokes the identity of the clone node in the network. The detailed algorithm for the proposed work is outlined below.

Max_dist =Node_speed × time_difference (Ti-T) (2)

3. Results and Discussion

A simulation of the proposed work is conducted within a network area of 600m × 600m, comprising 50 nodes randomly deployed. The GPSR routing protocol is employed for efficient transmission, reducing communication costs by establishing the optimal path between nodes. Each node utilizes the IEEE 802.11 medium access control protocol, and message broadcasting employs CBR traffic with a packet size of 1024 bytes.

To avoid unnecessary forwarding of claiming messages to all nodes in the network, the greedy perimeter forwarding technique [72] is employed. This technique significantly reduces communication costs and enhances the network throughput compared to the existing RDE scheme presented in [71], as illustrated in Fig. c and Fig. d.

Fig. c depicts the plot of node speed on the X-axis and the number of messages sent on the Y-axis for both RDE [71] and STBD. The speed varies from 10m/s to 50 m/s, with the number of messages sent increasing up to 40000. The graph demonstrates that the communication cost of the proposed algorithm is lower than that of RDE [71], resulting in energy savings for the nodes.

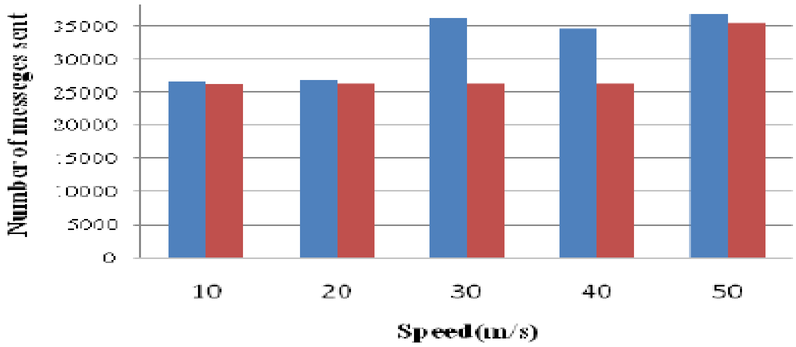


Figure c: Communication Cost

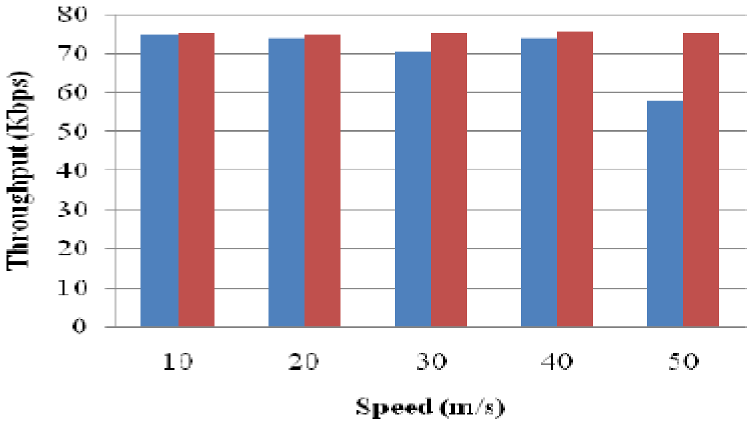


Figure d: Throughput

Fig. d illustrates the plot of node speed on the X-axis and throughput in Kbps on the Y-axis for both RDE [71] and STBD. Upon analysis, it is evident that the throughput of the proposed algorithm surpasses that of the existing RDE [71]-based approach.
Additionally, the Routing Overhead of the proposed STBD algorithm is lower compared to the existing RDE [71]-based detection, as depicted in Fig. e. Node speed varies from 10m/s to 50m/s on the X-axis, while routing overhead in terms of packets is shown on the Y-axis.

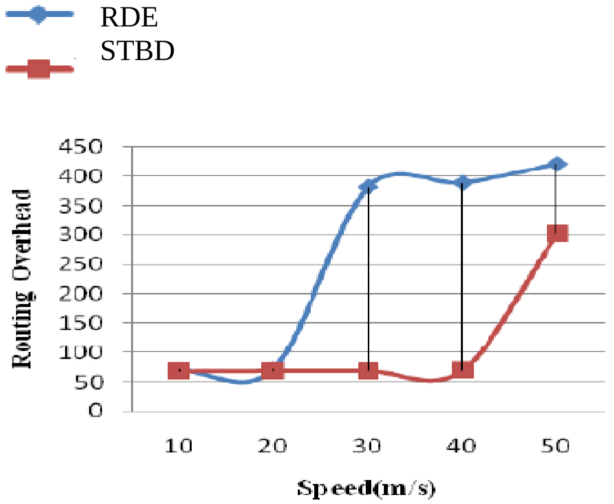


Figure e: Routing Overhead

4. Conclusion.

This document offers an summary of both surviving and freshly projected schemes for detecting duplicate strikes in HWSN. It thoroughly discusses and summarizes the strengths and weaknesses of these methods. The examination of joint reproduction outbreaks in the latest research sheds light on the comprehensive landscape of security threats within HWSNs. Resolving these security challenges is crucial for real-life implementation, emphasizing the importance of capable resources usage, low transmission budget, minimal retention requirements, and fast exposure. The paper provides a comprehensive perspective on node clone attacks in wireless sensor networks. Introducing a novel technique, STBD, for efficient duplicate attack recognition is a focal point. Simulation parameters include transmission cost, output, and directing transparency. Graphical representations clearly indicate that the STBD algorithm outperforms existing methods in clone detection.

References

I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," Computer Networks, vol. 38, no. 4, pp. 393–422, 2002.

H. Chan, A. Perrig, and D. Song, “Random key predistribution schemes for sensor networks,” in Proceedings of the IEEE Symposium on Security and Privacy, pp. 197–213, IEEE, May 2003.

W. T. Zhu, J. Zhou, R. H. Deng, and F. Bao, “Detecting node replication attacks in wireless sensor networks: a survey,” Journal of Network and Computer Applications, vol. 35,no. 3, pp.1022–1034, 2012.

C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,” Ad Hoc Networks, vol. 1, no. 2-3, pp. 293–315, 2003.

M. Luk,G.Mezzour, A. Perrig, andV.Gligor, “MiniSec: a secure sensor network communication architecture,” in Proceedings of the 6th International Symposium on Information Processing in Sensor Networks (IPSN ’07), pp. 479–488, IEEE, April 2007.

R. Poovendran, C. Wang, and S. Roy, Secure Localization and Time Synchronization: ForWireless Sensor and Ad hoc Networks, vol. 30, Springer, New York, NY, USA, 2006.

B. Sun, L.Osborne, Y. Xiao, and S.Guizani, “Intrusion detection techniques in mobile ad hoc and wireless sensor networks,” IEEEWireless Communications, vol. 14, no. 5, pp. 56–63, 2007.

W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. Abdelzaher, “PDA: privacy-preserving data aggregation in wireless sensor networks,” in Proceedings of the IEEE 26th IEEE International Conference on Computer Communications (INFOCOM’07), pp. 2045–2053, Anchorage, Alaska, USA, May 2007.

A. Perrig, J. Stankovic, and D. Wagner, “Security in wireless sensor networks,” Communications of the ACM, vol. 47, no. 6, pp. 53–57, 2004.

G. Kulkarni, R. Shelk, K. Gaikwad, V. Solanke, S. Gujar, and P. Khatawkar, “Wireless sensor network security threats,” in Proceedings of the 15th International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom '13), pp. 131–135, Bangalore, India, September 2013.

D. G. Padmavathi andM. Shanmugapriya, “A survey of attacks, security mechanisms and challenges in wireless sensor networks,” International Journal of Computer Science and InformationSecurity, vol. 4, no. 1, pp. 1–9, 2009.

A. K. Pathan, H.-W. Lee, and C. S. Hong, “Security in wireless sensor networks: issues and challenges,” in Proceedings of the 8thInternational Conference Advanced Communication Technology (ICACT ’06), vol. 2, pp. 1043–1048, Phoenix Park, Ireland, February 2006.

Y. Li, M. T. Thai, and W. Wu, Wireless Sensor Networks and Applications, Springer, New York, NY, USA, 2008.

B. Parno, A. Perrig, and V. Gligor, “Distributed detection of node replication attacks in sensor networks,” in Proceedings of the IEEE Symposium on Security and Privacy, pp. 49–63, IEEE, May 2005.

Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, “Randomwalk based approach to detect clone attacks in wireless sensor networks,” IEEE Journal on Selected Areas in Communications,vol. 28, no. 5, pp. 677–691, 2010.

A. Seshadri, A. Perrig, L. Van Doom, and P. Khosla, “SWATT: Softwarebased attestation for embedded devices,,” in Proceedings of the IEEE Symposium on Security and Privacy, pp. 272– 282, IEEE, May 2004.

F. Hu and N. K. Sharma, “Security considerations in ad hoc sensor networks,” Ad HocNetworks, vol. 3, no. 1,pp. 69–89, 2005.

D. Balenson, D. Carman, P. Dinsmore, and P. Kruus, “Communications security architecture for army sensor networks,” NAI Labs TR# 00-016, 2000.

A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, “SPINS: security protocols for sensor networks,” Wireless Networks, vol. 8, no. 5, pp. 521–534, 2002.

L. Zhou and Z. J. Haas, “Securing ad hoc networks,” IEEE Network, vol. 13, no. 6, pp. 24–30, 1999.

J. K. Liu, J. Baek, J. Zhou, Y. Yang, and J. W. Wong, “Efficient online/offline identity-based signature for wireless sensor network,” International Journal of Information Security, vol. 9, no. 4, pp. 287–296, 2010.

M. Zhang, V. Khanapure, S. Chen, and X. Xiao, “Memory efficient protocols for detecting node replication attacks in wireless sensor networks,” in Proceedings of the 17th IEEE International Conference on Network Protocols (ICNP ’09), pp. 284–293, IEEE, October 2009.

I. Amundson and X. D. Koutsoukos, “A survey on localization for mobile wireless sensor networks,” in Mobile Entity Localization and Tracking in GPS-Less Environments, pp. 235–254, Springer, 2009.

E. Ekici, Y.Gu, and D. Bozdag, “Mobility-based communication in wireless sensor networks,” IEEE Communications Magazine, vol. 44, no. 7, pp. 56–62, 2006.

S. A. Munir, B. Ren, W. Jiao, B. Wang, D. Xie, and J. Ma, “Mobile wireless sensor network: architecture and enabling technologies for ubiquitous computing,” in Proceedings of the 21st

International Conference on Advanced Information Networking and Applications Workshops/Symposia (AINAW'07), pp. 113–120, IEEE, May 2007.

S. Tilak, V. Kolar, N. B. Abu-Ghazaleh, and K.-D. Kang, "Dynamic localization control for mobile sensor networks," in Proceedings of the 24th IEEE International Performance, Computing, and Communications Conference (IPCCC '05), pp. 587–592, April 2005.

A.Kansal,A.A. Somasundara,D.D. Jea,M. B. Srivastava, and D. Estrin, "Intelligent fluid infrastructure for embedded networks," in Proceedings of the 2nd ACM International Conference on Mobile Systems, Applications and Services (MobiSys '04), pp. 111– 124, June 2004.

G. Song, Y. Zhou, Z. Wei, and A. Song, "A smart node architecture for adding mobility to wireless sensor networks," Sensors and Actuators A: Physical, vol. 147, no. 1, pp. 216–221, 2008.

S. R. Gandham, M. Dawande, R. Prakash, and S. Venkatesan, "Energy efficient schemes for wireless sensor networks with multiple mobile base stations," in Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '03), vol. 1, pp. 377–381, IEEE, December 2003.

J. W. Ho, M. Wright, and S. K. Das, "Fast detection of replica node attacks in mobile sensor networks using sequential analysis," in Proceedings of the 28th Conference on Computer Communications (INFOCOM '09), pp. 1773–1781, IEEE, April 2009.

J.-W. Ho, M. Wright, and S. K. Das, "Fast detection of mobile replica node attacks in wireless sensor networks using sequential hypothesis testing," IEEE Transactions on Mobile Computing, vol. 10, no. 6, pp. 767–782, 2011.

X.-M. Deng and Y. Xiong, "A new protocol for the detection of node replication attacks in mobile wireless sensor networks," Journal of Computer Science and Technology, vol. 26, no. 4, pp. 732–743, 2011.

C.-M. Yu, C.-S. Lu, and S.-Y. Kuo, "Mobile sensor network resilient against node replication attacks," in Proceedings of the 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '08), pp. 597–599, San Francisco, Calif, USA, June 2008.

[C.-M. Yu, C.-S. Lu, and S.-Y. Kuo, "Efficient and distributed detection of node replication attacks in mobile sensor networks," in Proceedings of the 70th IEEE Vehicular Technology Conference Fall (VTC '09-Fall), pp. 1–5, Anchorage, Alaska, USA, September 2009.

X. Deng, Y. Xiong, and D. Chen, "Mobility-assisted detection of the replication attacks in mobile wireless sensor networks," in Proceedings of the 6th Annual IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '10), pp. 225–232, IEEE, October 2010.

L.-M. Wang and Y. Shi, "Patrol detection for replica attacks on wireless sensor networks," Sensors, vol. 11, no. 3, pp. 2496–2504, 2011.

Y. Lou, Y. Zhang, and S. Liu, "Single hop detection of node clone attacks in mobile wireless sensor networks," Procedia Engineering, vol. 29, pp. 2798–2803, 2012.

C.-M. Yu, Y.-T. Tsou, C.-S. Lu, and S.-Y. Kuo, "Localized algorithms for detection of node replication attacks in mobile sensor networks," IEEE Transactions on Information Forensics and Security, vol. 8, no. 5, pp. 754–768, 2013.

W. T. Zhu, J. Zhou, R. H. Deng, and F. Bao, "Detecting node replication attacks in mobile sensor networks: theory and approaches," Security and Communication Networks, vol. 5, no. 5, pp. 496–507, 2012.

K. Cho, M. Jo, T. Kwon, H.-H. Chen, and D. H. Lee, "Classification and experimental analysis for clone detection approaches in wireless sensor networks," IEEE Systems Journal, vol. 7, no. 1, pp. 26–35, 2013.

R. Di Pietro, L. V. Mancini, C. Soriente, A. Spognardi, and G. Tsudik, "Catch me (if you can): data survival in unattended sensor networks," in Proceedings of the 6th Annual IEEE International Conference on Pervasive Computing and Communications (PerCom '08), pp. 185–194, Hong Kong, March 2008.

C.-M. Yu, Y.-T. Tsou, C.-S. Lu, and S.-Y. Kuo, "Constrained function-based message authentication for sensor networks," IEEE Transactions on Information Forensics and Security, vol. 6, no. 2, pp. 407–425, 2011.

F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," IEEE Journal on Selected Areas in Communications, vol. 23, no. 4, pp. 839–850, 2005.

L. Yu and J. Li, "Grouping-based resilient statistical en-route filtering for sensor networks," in Proceedings of the IEEE Conference on Computer Communications (INFOCOM'09), pp. 1782–1790, IEEE, 2009.

S. Zhu, S. Setia, S. Jajodia, and P. Ning, “An interleaved hopby- hop authentication scheme for filtering of injected false data in sensor networks,” in Proceedings of the IEEE Symposium on Security and Privacy, pp. 259–271, IEEE, May 2004.

H. Chan, A. Perrig, and D. Song, “Secure hierarchical innetwork aggregation in sensor networks,” in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS ’06), pp. 278–287, ACM, November 2006.

J.Deng, R.Han, andS.Mishra, “Security support for in-network processing in wireless sensor networks,” in Proceedings of the 1st ACMWorkshop on Security of Ad Hoc and Sensor etworks, pp. 83–92, ACM, October 2003.

B. Przydatek, D. Song, and A. Perrig, “SIA: secure information aggregation in sensor networks,” in Proceedings of the 1st International Conference on Embedded Networked Sensor Systems (SenSys ’03), pp. 255–265, ACM, November 2003.

Y. Yang, X. Wang, S. Zhu, and G. Cao, “SDAP: a secure hopby- hop data aggregation protocol for sensor networks,” ACM Transactions on Information and System Security, vol. 11, no. 4, article 18, 2008.

S. ˇCapkun, “Secure positioning in wireless networks,” IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 221–232, 2006.

S. Ganeriwal, S. Capkun, C.-C. Han, and M. B. Srivastava, “Secure time synchronization service for sensor networks,” in Proceedings of the ACM Workshop on Wireless Security (WiSe ’05), pp. 97–106, ACM, September 2005.

X. Hu, T. Park, and K. G. Shin, “Attack-tolerant time synchronization in wireless sensor networks,” in Proceedings of the IEEE Conference on Computer Communications (INFOCOM '08), Phoenix, Ariz, USA, April 2008.

Z. Li, W. Trappe, Y. Zhang, and B. Nath, “Robust statistical methods for securing wireless localization in sensor networks,” in Proceedings of the 4th International Symposium on Information Processing in Sensor Networks (IPSN ’05), pp. 91–98, IEEE, April 2005.

D. Liu, P.Ning, andW.K.Du, “Attack-resistant location estimation in sensor networks,” in Proceedings of the 4th International Symposium on Information Processing in Sensor Networks (IPSN ’05), pp. 99–106, IEEE, April 2005.

H. Song, S. Zhu, and G.Cao, “Attack-resilient time synchronization for wireless sensor networks,” Ad Hoc Networks, vol. 5, no. 1, pp. 112–125, 2007.

K. Sun, P. Ning, and C. Wang, “TinySeRSync: secure and resilient time synchronization in wireless sensor networks,” in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS ’06), pp. 264–277, November 2006.

J.N. Al-Karaki and A. E.Kamal, “Routing techniques in wireless sensor networks: a survey,” IEEEWireless Communications, vol. 11, no. 6, pp. 6–27, 2004.

M. Abolhasan, T. Wysocki, and E. Dutkiewicz, “A review of routing protocols for mobile ad hoc networks,” Ad Hoc Networks, vol. 2, no. 1, pp. 1–22, 2004.

W. Qin, M. Hempstead, and Y. Woodward, “A realistic power consumption model for wireless sensor network devices,” in Proceedings of the 3rd Annual IEEE Communications Society on Sensor and Ad hoc Communications and Networks (SECON ’06), pp. 286–295, IEEE, September 2006.

I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey,” International Journal of Computer and TeleCommunications Networking-Elsevier, 8(4), 393–422, March 2002.

Yanxiang Loua, Yong Zhanga, Shengli Liua, “Single Hop Detection of Node Clone Attacks in Mobile Wireless Sensor Networks”, International Workshop on Information and Electronics Engineering (IWIEE), 29, Pages 2798-2803, 2012.

R. Sivaraj and R. Thangarajan, "Location and Time Based Clone Detection in Wireless Sensor Networks," Fourth International Conference on Communication Systems and Network Technologies, Bhopal,pp.133-137, 2014.

H. Choi, S. Zhu, and T. F. L. Porta, “SET: Detecting node clones in sensor networks,” in Proc. Security Privacy Commun.Netw. Workshops, pp. 341–350, 2007.

Kwantae Cho, Minho Jo, Taekyoung Kwon, Hsiao–Hwa Chen, and Dong Hoon Lee, “Classification and Experimental Analysis for Clone Detection Approaches in Wireless Sensor Networks,” IEEE Sys. Journal., vol. 7, no.1, Mar. 2013.

B. Parno, A. Perrig and V. Gligor, "Distributed detection of node replication attacks in sensor networks," IEEE Symposium on Security and Privacy (S&P'05), pp. 49-63, 2005.

Y. Zeng, J. Cao, S. Zhang, S. Guo and L. Xie, "Random-walk based approach to detect clone attacks in wireless sensor networks," IEEE Journal on Selected Areas in Communications, vol. 28, no. 5, pp. 677- 691, June 2010.

W. Z. Khan, M. Y. Aalsalem, N. M. Saad, Y. Xaing and T. H. Luan, "Detecting replicated nodes in Wireless Sensor Networks using random walks and network division," IEEE Wireless Communications and Networking Conference (WCNC), Istanbul, pp. 2623-2628, 2014.

M. Conti, R. D. 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. 8thACMMobiHoc,Montreal, QC, Canada, pp. 80–89, 2007.

Sathish, R.; Kumar, D.R., "Dynamic Detection of Clone Attack in Wireless Sensor Networks," International Conference on Communication Systems and Network Technologies (CSNT), pp.501,505, 6-8 April 2013.

K. Farah and L. Nabila, "The MCD Protocol for Securing Wireless Sensor Networks against Nodes Replication Attacks," International Conference on Advanced Networking Distributed Systems and Applications, Bejaia, pp. 58-63,2014.

Zhijun Li and Guang Gong, "Randomly directed exploration: An efficient node clone detection protocol in wireless sensor networks," 2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, Macau, pp. 1030-1035, 2009.

Brad Karp and H. T. Kung. 2000. “GPSR: greedy perimeter stateless routing for wireless networks.” In Proceedings of the 6th annual international conference on Mobile computing and networking (MobiCom '00). ACM, New York, NY, USA, 243-254.

[A.Boonsongsrikul, S. Kocijancic and S. Suppharangsan, “Effective energy consumption on wireless sensor networks: survey and challenges,” IEEE Pub. pp. 469–473, May. 2013.

H. Choi, S. Zhu, and T. Laporta. Set: “Detecting node clones in sensor networks”. In SecureComm, 2007.

R. Sivaraj and R. Thangarajan, "Location and Time Based Clone Detection in Wireless Sensor Networks," Fourth International Conference on Communication Systems and Network Technologies, Bhopal, pp. 133-137, 2014.

Enebe, J. T. (2020). The Awareness and Uptake of Cervical Cancer Screening AmongFemale Nurses in Enugu, South-East, Nigeria. TEXILA INTERNATIONAL JOURNAL OF PUBLIC HEALTH, 8(2), 154–164. https://doi.org/10.21522/tijph.2013.08.02.art018

Reviewing Effectiveness of Artificial Intelligence Techniques Against Cyber Security Risks: In Case of It Industry in Saudi Arabia. (2020). Advances in Machine Learning &amp; Artificial Intelligence, 1(1). https://doi.org/10. 33140/amlai.01.01.05