Exploration of Detection Method of Clone Attack in Wireless Sensor Network

Sachin Lalar, Shashi Bhushan, Surender

Abstract*: Wireless sensor networks have a lot of sensor nodes that are small, cheap and resource-constraints, but are often used to perform various monitoring operations in unmanned and demanding environments. Networks are vulnerable to different application-based and application-independent attacks. We examine node replication attacks, which are typical threats in the sensor network. In this attack, the enemy generates its own sensor node using stealing sensor from network. The attacker physically occupies the node, takes his secret credentials, and duplicates a large number of nodes with some controlled counterparts. The defense against clone node attacks has become an important research element in the safety of the sensor network. In this study, we classify and examine the different proposals in each category. We also compare the memory and communication cost of different clone node detection approach.

***Keywords* : Wireless Sensor Network, Attacks, Clone Node Attack, Memory Cost, Communication Cost**

.

I. INTRODUCTION

Wireless Sensor Network (WSN) is a collection of sensor nodes, which has advanced network architecture with detection capabilities, limited resources [1]. WSNs are always distributed in difficult, hostile and unfavorable environments. The resistant hardware of node which is very sensitive can damage the sensor node. We will focus only on the most malicious attacks known as clone node attacks or node replication attacks. In this attack, the enemy physically grabs one or more sensor nodes and compromises their secret credentials. Then he creates a replica of the compromised node and runs it secretly in a strategic position on the network. Attackers can influence these clones and inject many internal attacks, misinformation and traffic such as black holes, wormhole attacks, selective forwarding attacks and DNS attacks. The clone node observes and listens to the nodes and cancels & blocks the traffic of other sensor nodes. There are some solutions of clone node attack in which we are not interesting for two main reasons. First of all, protecting all sensor nodes in a network with anti-tamper hardware is expensive and, secondly, it's expensive because qualified attackers can bypass tamper resistance. Therefore, it is necessary to develop software-based steps to identify clone nodes. This is because all the protocols currently available for authentication and secure communication can make them part of the network.

In the literature, two solutions i.e. centralized and distributed based on software firmware have been proposed to detect the vulnerability of node replication in WSN. In a centralized solution, the identification procedure is based on the base station or on the central auxiliary authority. In a distributed solution, the discovery process is performed without the central authority being included by all the central sensor nodes in the network. For example, structured WSN has many mobile sensor nodes, so more complex network security is required to stay connected and detect network failures. Indeed, the proposed methods in static WSNs are not directly applicable in the mobile WSN. This paper focuses on node replication or clone attacks on SWSN and MWSN. The clone attack is generally considered a security threat independent of the application. In this case, the sensor node is completely proscribed by the attacker on the network and is considered a real or legitimate sensor node. In Clone Attack, then attacker copies the root node from the network or system, using confidential information such as code, identification and encryption resources and sends these clone nodes to the network. The attacker controls the same or the entire network communication, controls the WSN, inserts incorrect information, interrupts the signal, modifies the cluster structure, runs various protocols and disables the WSN performance. Furthermore, due to the dangerous nature of tumors and the speed of tumors within the MWSN, the clone is very difficult to identify and the difference between legal and illegal cancers is difficult. According to Perno et al. Consultants based on sensor node information, stored data and memory (such as ID, key or stored code), many replicas use the tools available to quickly resolve the node. As indicated above, the mobility of the MWSN node adds complexity to a stable WSN, making it more difficult to detect the duplication of the MWSN node or the clone attack than the traditional WSN. Previously, we examined the security risks of other clone attacks and existing detection methods. We will examine the various advantages and disadvantages of mobile WSN clone detection methods.

The purpose of paper is examined the various mobile WSN clone detection methods and analyze their performance in ns2 simulator.

Revised Manuscript Received on November 15, 2019.

***** Correspondence Author

Sachin Lalar*, Ph.D. Research Scholar, CSE, IKGPTU, Kapurthala, India. Email: sachin509@gmail.com

Shashi Bhushan, Professor, I.T., CGC, Landran, Punjab, India. Email: shashibhushan6@gmail.com

Surender, A.P., Computer Appl GTB, Bhawanigarh, India. Email: ssjangra20@rediffmail.com

The paper is structured in five sections as: The 2nd Section illustrates the Clone Node Attack in mobile sensor network. After that the Section 3rd describes various clone node detection methods in wsn. Section 4 simulates the various mobile clone detection methods in ns2 and discusses the result. The last section presents the conclusion.

II. CLONE NODE ATTACK

A specialized group of sensor which performs the various detection operations is called Wireless Sensor Network (WSN). Today, WSN is a key and important aspect of the research field. By creating more communication channels, mobility allows data integrity and the capacity of large channels, reducing the number of hop messages. Sensor nodes are generally distributed in meteorological points to create a multi-hop mesh system scheme. Each network of sensor nodes has a peer-to-peer function that collects messages and provides routing information to the base station. A mobility node is really good sensor nodes which not only perform the detection operations, but also maintain a flexible and manageable automatic information base. The base station is maintained to the connection to another network or system, such as the Internet [2]. Mobility allows sensor nodes to trace movement mechanisms (chemical cloud, transport, baggage, etc.). One of the applications of Mobile Wireless Sensor Network (MWSN) is use in detection of fire. MWSN observes fires in which mobile sensors can follow and exit when a fire develops. The mobile sensor node has the ability to maintain a safe firing range, also indicating where the border is at a given time and updating the fire brigade. Fig. 1 shows the replication process on MWSN, ie how an attacker compromises the mobile node, alters the information and sends it back to the network for malicious activity. Red node indicates the presence of a replica and the MWSN replication node is considered mobile. Therefore, due to the mobility characteristics, it is very difficult to isolate the original MWSN node.

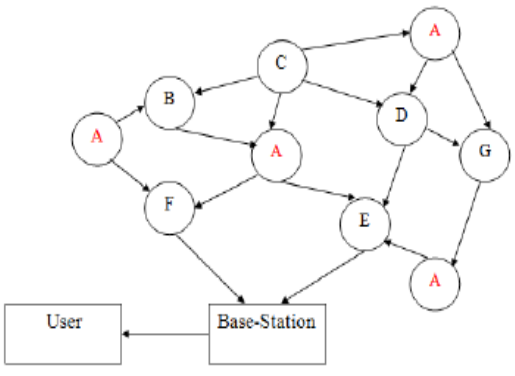

Fig. 1: Clone Node Attack example [22]

A diagram of a wireless sensor network is presented in Figure 1. In this figure, clone node A replicates on the network. Node A can communicate to neighboring nodes in the network. Clone knots cause various attacks within network. Clone node A can receive a valid packet from a legitimate node and discard the packet. Therefore, packet retransmission affects network performance. In Section 4 we will use the ns2 simulator to see the effects of the clone node in wsn. The next section describes the various attacks initiated by the clone node.

III. CLONE NODE ATTACK DETECTION SCHEME

Several methods have been suggested to detect intruders of stable WSN clones and fall into two main types: centralized and distributed. Base stations are seen as a powerful center for merging information and central to decision making. In the identification process, each node of the network sends its position request (ID, location information) to its base station (sink node) from its neighbors [3]. After receiving all the position requests, the base station checks the node ID and its location and, if it detects two different positions with the same ID, generates the clone node alarm. The distributed method provides a special validation method called Clamor-Reporter-Witness where there is no central authority and locally distributed nodes send location IDs to randomly selected nodes instead of the base station (sink). In general, research methods can be divided into two main categories: centralized and distributed. These two methods are described in detail in the following subsections.

A. Clone Node Detection Approach in Static Sensor Network

Author [4] proposed a cloned key detection protocol in terms of probability key distribution. The basic idea is that the keys used according to the distribution scheme of random key assumptions must adhere to a specific schema and can be duplicated beyond the usage limit. This protocol uses the bloom filter calculations to collect key usage statistics. Each node calculates a key bloom filter used to communicate with neighboring nodes. Add a random (meaningless) number to the bloom filter and encrypt the result using the base station's public key. This encrypted data structure is transferred to the base station.

Author [5] proposed to find a clone in a sensor network called Center. With SET, the network is randomly divided into distinct subsets. Each subcommittee has a subset leader and members leave the subset leader. Multiple sources are assigned to create multiple substructures of side effects, with each subset being a node in the substructure. Each member of the subcommittee collects information and forwards it to the source of the substructure. To identify replicating nodes, intersection operations are performed on each element of the substructure. If all subsets of the sub-tree have the empty intersection, this sub-tree does not contain clone nodes.

Author [6] proposed to detect the clone attack in real time. In their approach, each sensor is calculated by inserting the fingerprint in the S-code overlaps the information in the vicinity. Each node stores the fingerprints of all the neighboring nodes. Every time a node sends a message, the message must include a fingerprint.

Can check fingerprints on neighbors. Since fingerprints do not belong to the same "community", messages sent from cloned nodes distributed elsewhere are identified and eliminated. The motivation behind the plan to detect a clone attack is to examine the social characteristics of each sensor. When distributed, these sensors live in a fixed environment. The sensor and its surroundings form a small "community" or "social network".

The study by Author [7] proposed a hierarchical distribution algorithm based on the selection of the cluster head in which a network can detect the attacks of the node clone using a bloom filter mechanism. More precisely, the local negotiation algorithm depends on the selection of the cluster head performed using the LNCA (Clustering Algorithm) protocol. Each head cluster exchanges the ID of the member node with another head cluster through a bloom filter to identify the clone of the node. The algorithm works in three steps. All the materials necessary for the calculation of the first stage flowering filter and the cryptographic operation performed on a pre-distributed network of each sensor node. In the second phase, the cluster head selection is made. In the third step, the bloom filter architecture is performed by each cluster head and the bloom filter is validated by the other cluster heads.

Author [8] proposed a central mechanism called compressed detection based clone identification (CSI) for a network of static wireless sensors. The idea behind CSI is that each node sends fixed probe data (α) to the neighbor hop. By compressing the method of data collection based on detection, the composite nodes are obtained from the direct and aggregate number of derivation nodes. The base station (BS) at the base of the aggregation tree receives complete results and the network receives valid data. As a result of the reboot, a non-clone node can report a number only once, so nodes with a sensitivity value greater than node consider a clone.

On the protocols N2NB and DM are suggested by [9]. Both protocols received little attention. In N2NB, each node fills the entire network with a standardized transmission and requires its own location (not the neighbors). Each node stores location information in the adjacent node, which has a value. Each node that receives a conflicting complaint runs a policy to back up the problematic node and eventually the clone is disconnected from the adjacent node (this separates it from the WSN). If network size B is assumed, the N2NB protocol reaches a 100% detection rate until the transmission reaches each node and some simulations are performed so that each node sends a specific message only once. The suppression algorithm is used. The DM protocol is a good example of a client-reporter-witness framework specification. The seed is a node that sends the message to the neighbors locally and each neighbor acts as a reporter and uses the function to map the client ID on the monitor. He then forwards the request to the nearby mirror witness and receives two different position requests with the same node ID if the enemy duplicates the node. One problem is where the attacker's abilities can be used to find a witness with a specific client ID and if the attacker's clone can be identified and compromised before entering the WSN.

Two other distributed algorithms have been introduced to detect clone nodes in wireless sensor networks [10]. This is a more mature plan than the DM. The first protocol, called Randomized Multicast (RM), distributes the position claims to randomly selected monitoring nodes. The second protocol, Line-Selected Multicast (LSM), uses the routing topology of the network to select the monitoring of the position of the nodes and uses the geometric probabilities to identify the clone nodes. In RM, each node sends a position request to a neighbor of 1 hop. Then each neighbor randomly selects the monitoring node in the range and uses geographical routing to forward the position request with the node potential closest to the selected location. According to the birthday paradigm, if there are duplicate nodes in the network, at least one monitoring node could have conflicting position claims. The main objective of LSM is to reduce the cost of communication and increase the likelihood of investigation. In addition to storing position requests on randomly selected monitoring nodes, the intermediate nodes also monitor the nodes for forwarding position requests. The lines appear to be randomly drawn on the network and the two intersecting lines are test nodes that receive conflicting position claims. Authors [11] have established the WSN against the infiltration of node clones using a symmetric polynomial to establish coupled keys and for propagation models based on groups defined by the polynomial. The installation of sensors is in the groups. Each node belongs to a different generation. In that plan, only the newly distributed nodes can set the neighbors and pair the keys and know the highest generation number that runs all the nodes in the network. Therefore, the distribution of the clone node is obsolete and therefore cannot establish the key to be coupled to the neighbor.

A randomized and efficient distributed protocol called RED [12] has been proposed to detect intruders of the node Clone. It can be implemented in two fixed-time steps. In the first step, the random value is shared by the base station among all the nodes. The second phase is called the investigative phase. During the survey phase, each node sends its complaint (ID and position) to the nearest node. Each node (with probability) sends this request to a range of pseudo-randomly selected network locations. Replication uses the random function as input ID, a random number, and so on.

According to Author [13] suggests two delivery protocols for detecting node clone attacks, known as single decay cells (SDCs) and parallel multiple probability cells (P-MPC). With both protocols, the entire sensor network is divided into cells, which form the geographical grid. In SDC, each node ID is individually mapped to a single grid cell. When the search process is performed, each node sends a position request to the nearest node.

Each adjacent node then advances the claim of position with the potential of a particular cell by executing a geographic hash function using the input ID. When the target cell node receives a position request, it fills the position request for the entire cell. Each node in the target cell stores the position complaint with probability. Therefore, since the position argument of the clone node is transferred to the same cell, the clone node can be satisfied with a certain probability.

Author [14] proposed a key pre-distribution as S-temporal combination based on polynomials for wireless sensor networks, which integrates the key content of the node with the time and location of distribution. In PSPP, node key information works only in the first distribution area. If the node leaves the distribution path, the key information is invalid. Using this idea, their plan provides resistance to clone attacks.

Author [15] proposed a real-time neighbor (NBDS) detection scheme for attacking the node clone in wireless sensor networks. The main idea of his plan is that when a person goes to another community, he meets a new neighbor and tells them where the new neighbor comes from. Ho [16] proposed a method for detecting node capture for wireless sensor networks. Their plan is to detect the sensor nodes acquired by sequential analysis. It uses the fact that a node that is physically occupied does not exist in the network from the moment of acquisition to the rearrangement. Therefore, the nodes acquired during that period do not participate in the functioning of the network. With this intuition, the acquired nodes can be detected using a test of the sequential probability ratio (SPRT). The protocol measures first the duration in which the sensor nodes are not and therefore compares them with a predetermined threshold. If the threshold is exceeded, the sensor node is considered a kernel node. The effective node capture detection function is based on the configured threshold.

According to Author [17], a distributed and critical approach is provided to detect a clone attack. These plans work in three phases: start-up, monitoring of the node identification phase and node withdrawal phase. In the pre-implementation phase, the base station (BS) integrates a specific position coordinate (hereinafter known as probe point, VP) with each node ID using the geographical hash function

B. Clone Node Detection Approach in Mobile Sensor Network

Mobility has become an important research area for the WSN community. In the mobile WSN, mobility plays an important role in the implementation of the application since the distribution of mobile entities can solve many problems and offer many advantages compared to a stable WSN. The node clone detection technology developed for the stable WSN will not work for the mobile WSN since it will not work if the mobile node is supposed to proceed as the mobile WSN. As a result, many methods (not yet fully mature) have been developed for the mobile WSN to detect clones or clone nodes.

Ho et al. [16] proposed a scheme for detecting mobile clones based on a test of the sequential probability ratio (SPRT). Their protocol is based on the fact that imaginary mobile nodes should not proceed faster than the maximum system configuration speed. Consequently, as long as the speed measurement system is used with the lowest error rate, the node of the imaginary (native) mobile sensor seems to be the maximum speed of the system configuration.

Author [18] proposed a new protocol to detect clones in the mobile WSN. They used the idea of multidimensional coupling of pre-distribution and key bloom filters. This ensures that the clone is not on the actual identifier and collects the number of torque keys installed by each sensor node. Clones can be tested to see if the number of torque keys they install exceeds the limit. The protocol works in three phases: initialization of the node, installation and identification in pairs.

According to Author [19] proposed a protocol for detecting a node clone attack known as single-hop detection (SHP) for mobile wireless sensor networks. The SHD protocol takes advantage of the fact that a physical node (or equivalent node ID and private key) is not always visible to another nearby community. Otherwise, the network must be cloned. The neighboring node community is regularly characterized by a list of nodes near a hop available on WSN, since sensor nodes must know their neighbors to communicate with each other.

According to Author [20] proposed two clone detection algorithms for mobile sensor networks. The first algorithm is a token-based authentication scheme suggested to detect clone vulnerabilities and clones do not work together (in the case of non-attachments). For clones that interact effectively with each other, a random encounter between the identification method and the statistics-based physical nodes is proposed. In the first algorithm, the base station periodically sends a secure timestamp throughout the search field through the broadcast authentication protocol. The transmission signals the start of the investigation round.

Author [21] proposed two algorithms to detect node acquisition vulnerabilities in a network of mobile wireless sensors. Their first algorithm was Simple Distribution Detection (STD), which allowed attackers to search only local information on the node. Another algorithm, called Cooperative Distribution Detection (CDD), offers the advantage of collaboration between nodes to improve search performance.

Author [17] suggested two schemes for detecting node clone vulnerabilities in a network of mobile wireless sensors. The first is called Unary Time Location Storage and Exchange (UTLSE) and the second is called Multi-Time Location Storage and Definition (MTLSD). With both protocols, after receiving the statements that time has passed, the witness speaks to the network instead of transmitting these arguments. This means that data is transmitted only when the right witnesses meet.

When two nodes come together, they exchange time requests. That is, if the Tracer track receives a time request from a neighbor, the inspector does not immediately send this time request to the monitor. At the moment it is not within range of communications, but will defend the charges for that place until the witness is confronted.

IV. COMPARISON OF CLONED ATTACK DETECTION APPROACHES AND SIMULATION RESULT

All existing criteria for detecting replication attacks have some limitations that affect their functionality. Some limitations of the original method are highlighted here and are summarized as a table for comparison. Table 1 provides a comparative overview of all MWSN detection methods for communication costs, memory costs, rapid detection and NDFD parameters (non-terminal and fully distributed). Each solution for identifying the replication node comes with its own diagnostics, inspiration and technology and each plan has several positive and negative aspects. Based on this, we cannot say what the best strategy is. MWSN security is a big problem and must be identified quickly and effectively to manage the replication of a node. Otherwise, an attacker can easily capture or monitor the entire network and use it for malicious activities. As mentioned in the previous section, the central method (ie SPRT and new protocols) is based on the base station. The centralized approach has the advantage of a distributed method (SPRT method) able to detect images more quickly because it is based exclusively on punctual verification. This is a disadvantage, even in the case of a single point of failure. Authors propose a rapid analysis of the sequence of detection of node replication attacks (SPRT).

Basically, these approaches are based on the fact that the speed of the original mobile node should not exceed the maximum speed of the system and that replication moves very quickly and needs to be replaced. Therefore, if the speed of the mobile node exceeds the system speed, MWSN has two nodes with the same ID. SPRT depends on the hypothesis of the hierarchy of speed controls for each mobile node. This can be copied when the specified threshold is exceeded. Replicas are also considered mobile because they can adapt to some extent. Furthermore, speed measurement tools are expensive and cannot be easily implemented in the network. In [9], the author proposed a new protocol for detecting MWSN node replication attacks. Their theory is based on the idea of bloom filters and pre-distribution based on pairs of polynomial keys, explaining the belief that not all coupled nodes and side keys can be copied. If the number of pairs exceeds the number of clones, the threshold is checked to find the pair. This new replication detection protocol is another central way that a replication node cannot verify that the key communicates on the base station and if the value exceeds a certain threshold, the root node can be very damaging to the network. It is also necessary to identify replicas by observing false positives and false negatives. We suggest a distributed approach to solve a single point of failure. The most efficient survey (XED) has been proposed and its operating principle is based on the idea of exchanging random numbers in different places (remembering strategy and challenge). Therefore, if the mobile node does not exchange the correct random number or if the numbers do not match, a network replica is guaranteed. XED is based on a one-to-one node assembly and exchanges a random number, so it cannot be detected quickly. This process can delay the investigation process and be dangerous for the network because it can be vulnerable to intelligent attackers. As described in [20], since replication can easily set up a secret node and has a cellular formative function, it cannot communicate with the mobile node and can exist in the network.

The EDD system is based on two phases: offline and offline. The first pass is performed before distribution and the second pass for each mobile node in each movement. Seed approaches have been proposed to eliminate EDD archiving overheads and durability problems. Thus, each mobile node monitors only a subset of all optional nodes for a limited period of time. The EDD approach is based on the assembly of the node and on the maximum memory to store the information. This does not apply to real large network views. SEDD, on the other hand, regulates memory problems for the monitor, but requires more storage space. Furthermore, since these two nodes depend on each other's cactus time, they cannot be detected immediately.

A. Simulation and Result

In this section, we will implement the various clone node attack detection methods in the NS2 simulator. For this purpose, in each scenario the simulation is performed within 1000 seconds using the NS-2 simulator. The areas covered by static and mobile WSN are respectively 1000m x 1000m and 500m x 500m and communication range is 150m. The random movement process is repeated during the simulation period.

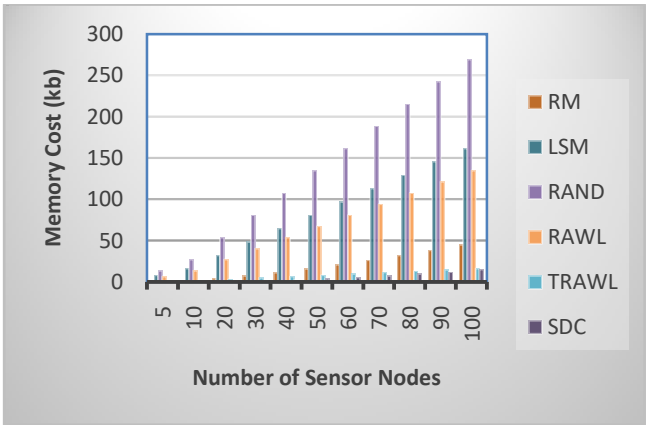

Fig. 2: Comparsion of Memory Cost

To test the detection scheme in the same simulation environment used in [10] and [11], identify single-node replicas (two clones replicated from the same real node) and simulate them with more than 10 simulation experiments.

Table- I: Comparison of Clone Node Detection Schemes

Method Name	Type of Network	Detection Approach Used	Memory cost	Communication cost	Pros	Comments
Random key distribution	Centralized Static Sensor Networks	Random key and Hypothesis test	--	O(n log n)	Highly Secure	Minimize vulnerability
CSI	Centralized Static Sensor Networks	Speed Measurement test	O(n)	$O(n\log n)$	Low Communication burden	Applicable in mobile WSN
SPRT	Distributed Mobile Sensor Networks	Speed Measurement test	$O(n)$	$O(n\sqrt{n})$	Low Overhead	Applicable in mobile WSN
SHD	Distributed Static Sensor Networks	Fingerprinting approach	O(p.g.d)	O(d.n. $\sqrt{n}$.g.p)	High rate of detection	Decreasing mobility
ABCD	Distributed Static Sensor Networks	Area and clustering based	O(n)	O(n log n)	Overhead High	Single point of failure
Hierarchical	Centralized Static Sensor Networks	Cluster head-based techniques	O(t)	$O(t^2)$	Low communication overhead	High detection rate
RED	Distributed Static Sensor Networks	Random value generation	O(p.g.d)	O(d.n. $\sqrt{n}$.g.p)	Average storage overhead	witness nodes Random generated
RAWL, TRAWL	Distributed Static Sensor Networks	Random walk approach	O(1)	O($\sqrt{n}$ log n)	Lowest overhead	Increase detection rate
XED	Distributed Mobile Sensor Networks	Remembered and Challenge	O(n)	O(1)	Constant Communication cost	Detection in mobile WSN
ZBNRD	Distributed Mobile Sensor Networks	Zone based detection	O(d)	O(n$\sqrt{n}$)	Decreased memory overhead and complexity	Dynamic detection of replicas
GDL,RMC	Distributed Mobile Sensor Networks	Intersection among cells	O($n^{0.5}$)	O($\sqrt{n}$ *$\sqrt{}$ m)	High detection rate and less energy consumption	Approach is used for uniform environment
NI-LEACH	Distributed Mobile Sensor Networks	Clustering based Intrusion detection	O (k.e)	O(l(1+m'2))	Balanced throughput, more secure, less delay	do not detect in case of multiple adversaries
Matrix and Bloom filter based	Distributed Mobile Sensor Networks	Matrix decomposition and bloom filter mechanism	O (n)	O (n log n)	Low storage overhead	Less resources consumption
LEACH-C	Distributed Mobile Sensor Networks	Enhanced LEACH Clustering based	---	---	Low energy consumption	Detect even the whole replicated cluster
X-RED	Distributed Mobile Sensor Networks	Dynamic detection and time variance based	__	__	High detection probability	High Traffic overhead

Method Name	Type of Network	Detection Approach Used	Memory cost	Communication cost	Pros	Comments
SET	Centralized Static Sensor Networks	Base station based	$O(d)$	$O(n)$	Storage Overhead low	Base Station Overload
N2NB	Distributed Static Sensor Networks	Node-to-network broadcasting	$O(1)$	$O(n2)$	More efficient than centralized approach	High communication overload
DM	Distributed Static Sensor Networks	Witness node	$O(g)$	$O(g\log\sqrt{n}/d)$	Communication overhead is reduced	Depend on Witness Node
RM	Distributed Static Sensor Networks	Witness node	$O(\sqrt{n})$	$O(n2)$	Witness nodes are randomly Selected	Lower detection probability
LSM	Distributed Static Sensor Networks	Witness node	$O(\sqrt{n})$	$O(n\sqrt{n})$	Reduced the communication overhead caused by RM.	Depend on Witness Node
SDC, P-MPC	Distributed Static Sensor Networks	Witness node	$O(\omega)$	$O(r \cdot \sqrt{n}) + O(s)$	More efficient then LSM	Dependant on cell size
RDE	Distributed Static Sensor Networks	Witness node	$O(\omega)$	$O(r \cdot \sqrt{n}) + O(s)$	Good memory overhead	Dependant on Network Topology
B-MEM	Distributed Static Sensor Networks	Witness node	$O(tk + t'k\sqrt{n})$	$O(k \cdot n \cdot\sqrt{n})$	Depend on Witness Node	Average Detection probability
Melchoretal.	Distributed Static Sensor Networks	Witness node	$O(d)$	$O(\sqrt{n})$	Low Storage Cost	Average Detection probability
Deng and Xiong scheme	Distributed Mobile Sensor Networks	Key usage based	—	$O(n\log n)$	Depend on Key	High Communication Cost
EDD	Distributed Mobile Sensor Networks	Node meeting based	$O(n)$	$O(1)$	Average Detection probability	High Computation Overhead in online Phase
SEDD	Distributed Mobile Sensor Networks	Node meeting based	$O(\xi)$	$O(n)$	Average Detection probability	High Computation Overhead
Wang Base Station	Distributed Mobile Sensor Networks	Mobility assisted based	—	$O(n)$	Low Storage Cost	Depend on base station
Wang without Base Station	Distributed Mobile Sensor Networks	Mobility assisted based	—	$O(n * \sqrt{k})$	Low Storage Cost	Communication Cost is High
UTLSE & MTLSD	Distributed Mobile Sensor Networks	Mobility assisted based	$O(\sqrt{n})$	$O(n)$	Low Storage Cost	Detection Probability is high

To compare clone detection method, we have used two parameters- Communication Cost and Memory cost. Fig 2 shows the result of memory cost of RM, LSM, RAND, RAWL, TRAWL and SDC clone detection method. The entire network was discovered by a stable WSN created by a similar random expansion of the network. The six schemes of the clone detection methods have different memory cost. We have simulated the result by varying the number of nodes in the network from 10 to 100. Fig. 2 shows that the memory cost of RAND is the highest out of the six methods and SDC method is the lowest. Fig. 3 shows that the communication cost of SDC is the lowest out of the six methods and RAND method is the highest. There are different patterns, the total memory uses are different for, we can easily find and use to consider. For example, a clone of RM costs can cure others, as long as it costs to identify most of the time taken for completion. That is, the less time it takes to plan a clone search, the more energy is saved.

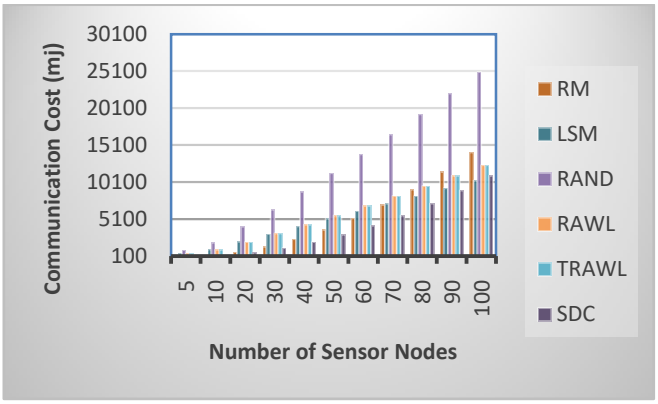

Fig. 3: Comparison of Communication Cost

V. CONCLUSION

The paper describes the different schemes for detection of clone nodes. The existing methods are widely categorized in distributed and centralized. Both classes of projects are specialized in detecting and preventing clone attacks, but both plans have some significant disadvantages. However, current research highlights the fact that there are still many challenges and problems that need to be addressed in order to make clone detection methods more suitable for real-world situations and to be accepted by sensors with limited resources. In this paper, various clone detection schemes have been simulated and evaluated with the following performance metrics: total communication and memory cost. The performance of SDC is better in both cases. Since the sensor is not tamper-proof hardware, it is important to provide a detection system against clone attack. The future work is to enhance the SDC protocol using fuzzy logic and the performance will be compared between the existing system and the enhanced system.

REFERENCES

1. Sachin Lalar, S Jangra, S Bhushan, "Study of Attacks & Countermeasures on Layers of Wireless Sensor Networks", International Journal of Control Theory and Applications, 2017; 10(15): 153-162
2. I. Akyildiz, S. Weilian,Y. Sankarasubramaniam & E. Cayirci, "A survey on sensor networks", *IEEE Communications Magazine, 40*(8), pp 102-114, 2002
3. H.C.Chaudhari and L.U. Kadam , "Wireless Sensor Network Security Attack and Challenges", International Journal of Networking, pp-04-16, 2011
4. B. Parno, A. Perrig, and V. D. 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.
5. H. Choi, S. Zhu, and T. F. L. Porta, "SET: Detecting node clones in sensor networks," in Proc. Security Privacy Commun. Netw. Workshops, 2007, pp. 341–350.
6. 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, 2010.
7. B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, "Localized multicast: efcient and distributed replica detection in large-scale sensor networks," *IEEE Transactions on Mobile Computing*, vol. 9, no. 7, pp. 913–926, 2010. A.D. Wood, J.A. Stankovic, and S.H. Son,"Jam: a jammed-area mapping service for sensor networks", Real-Time Systems Symposium, RTSS 2003. 24th IEEE, pages 286-297,2003
8. B. Zhu, V. G. K. Addada, S. Setia, S. Jajodia, and S. Roy, "Efficient distributed detection of node replication attacks in sensor networks," in *Proceedings of the 23rd Annual Computer Security Applications Conference (ACSAC '07)*, pp. 257–266, IEEE, Miami Beach, Fla, USA, December 2007.
9. Kwantae Cho, Minbo Jo, Member , IEEE, Tackyoung Kwon, Hsiao - Hwa Chen, Fellow, IEEE ,and Dong Hoon Lee, Member, IEEE" Classification and Experimental Ana;ysis for Clone Detection Approaches in Wireless Sensor Networks" IEEE SYSTEM JOURNAL.
10. M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, "Emergent properties: detection of the node-capture attack in mobile wireless sensor networks," in *Proceedings of the 1st ACM Conference on Wireless Network Security (WiSec '08)*, pp. 214–219, April 2008.
11. 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
12. 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, IEEE, San Francisco, Calif, USA, June 2008
13. Y. Lou, Y. Zhang, and S. Liu, "Single hop detection of node clone attacks in mobile wireless sensor networks," in *Proceedings of the International Workshop on Information and Electronics Engineering (IWIEE '12)*, pp. 2798–2803, Harbin, China, March 2012.
14. W. Z. Khan, M. Y. Aalsalem, M. N. B. M. Saad, and Y. Xiang, "Detection and mitigation of node replication attacks in wireless sensor networks: a survey," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 149023, 22 pages, 2013
15. K. Xing, F. Liu, X. Cheng, and D. H. C. Du, "Real-time detection of clone attacks in wireless sensor networks," in Proc. ICDCS, 2008, pp. 3–10.
16. 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 (IEEE INFOCOM '09)*, pp. 1773–1781, IEEE, Rio de Janeiro, Brazil, April 2009
17. B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in Proc. IEEE Symp. Security Privacy, May 2005, pp. 49–63.
18. R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, "On the detection of clones in sensor networks using random key predistribution," IEEE Trans. Syst. Man Cybern., vol. 37, no. 6, pp. 1246–1258, Nov. 2007.
19. M. Conti, R. 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. ACM Int. Symp. Mobile Ad Hoc Netw. Comput., 2007, pp. 80–89.
20. Z. Li and G. Gong, "DHT-based detection of node clone in wireless sensor networks," in Proc. 1st Int. Conf. Ad Hoc Netw., 2009, pp. 240–255.
21. C. A. Melchor, B. Ait-Salem, P. Gaborit, and K. Tamine, "Active detection of node replication attacks," Int. J. Comput. Sci. Netw. Security, vol. 9, no. 2, pp. 13–21, Feb. 2009.

22. Sachin Lalar, Shashi Bhushan & Surender, “An efficient tree-based clone detection scheme in wireless sensor network”, Journal of Information and Optimization Sciences, 40:5, 1003-1023, 2019.

AUTHORS PROFILE

Sachin Lalar is currently pursing Ph.D in the field of Wireless sensor network from IKGPTU, Kapurthala. He has been completed M.Tech from PEC Chandigarh. He has 10 years of teaching experience. He has published 12 research papers in various referred journals.

Dr. Shashi Bhushan has been working as Professor in the department of Information Technology, CGC Landran. He pursued his Ph.D from NIT Kurukshetra. He has more than 16 years of teaching experience. He had published more than 50 research papers in reputed journals and conferences including IEEE conferences.

Dr. Surender completed his M.Tech degree in Computer Science and Engineering from Ch. Devi Lal University Sirsa (Hry) in 2006, Ph.D in Computer Science and Application from Kurukshetra University, Kurukshetra in 2011.. He has more than 10 years teaching. Recently he is working as an Assistant Professor, in the Department of Computer Science, at GTB College, Bhawanigarh (Sangrur), Punjab, India. He has published over 50 publications in different International Journals and Conferences of repute.