Perlustrate of Detection Methodology against Clone Attacks in Wireless Sensor Networks

J. Sybi Cynthia
Department of Electronics & Communication
C.S.I. Institute of Technology, Thovalai
Tamil Nadu, India
sybi.cynthia@gmail.com

D. Shalini Punithavathani
Department of Computer Science
Government College of Engineering, Tirunelveli
Tamil Nadu, India
shalini329@gmail.com

***Abstract*- Wireless Sensor Networks (WSNs) is a capable technology and have immense potential to be employed in decisive situation like battle field and commercial application such as construction, traffic observation, environment monitoring and numerous other scenarios. One of the major challenges WSNs faces today is security breaches. A network security is very much necessary to face these security breaches. The WSN deployed in aggressive environments are susceptible to clone attacks. Clone attack would be probably be the most vigorous adversary in WSN especially in battlefield. And is waking up, belatedly, to the threat of an clone in wsn. It should be better organized for the research community to develop new architectures, systems and applications, and to assess alternatives and tradeoffs in developing technologies for its successful deployment. This paper is well emerge naturally in response to survey on various detection methodology and its evaluation metrics based on security primitives against clone attack in WSN. This paper promises many benefits for the research field in advance.**

Keywords- Clone Attacks, Network Security, Wireless Sensor Networks.

I. INTRODUCTION

Wireless communication networks are the preferred technology compared to the wired network as it offers more flexibility and lower cost for installation and commissioning. Wireless Sensor Network (WSN) consists of spatially distributed autonomous sensors to monitor corporal or ecological environment, such as temperature, sound, vibration, pressure, movement or contaminant and to considerately go by their data to a major location in the network. The emerging field of wireless sensor network comprises of sensing, computation, and communication into a single tiny device [1]. It consists of small nodes with sensing, computation, and wireless communication capabilities. A large number of these sensors can be networked in many applications that require unattended operations, hence producing a WSN [2]. It is not possible to protect anything unless one clearly understands what is to be protected. A specialized field in computer networking involves securing a computer network infrastructure which is typically handled by a network administrator or system administrator who is responsible for security policy, network software and hardware. Things that are considered for a test bed are servers, workstation, storage systems, routers, switches, etc.

Threats are of various types and it includes viruses and attacks. If someone tries to breach the security we call such an event as attacks. Network security is concerned with protection, integrity, confidentiality and availability of information. The security trinity involves prevention, detection and response [3]. As it has been said prevention is always better than cure, it is therefore essential to take necessary action to prevent an attack quite respond after attack. Similarly detection should be done as quickly as possible before the attack cause large damage in a network making it an irreversible process. Even if we lack in prevention and detection, the response should be immediately with necessary action like revoking process etc. There are number of applications of WSNs such as military and civil applications, target field imaging, intrusion detection, climate monitoring, protection and deliberate surveillance, etc [4]. Security breaches of the system means the illegal acquirement of unencrypted computerised data that comprises the security, confidentiality, or integrity of concealed information preserved by an individual or a commercial entity. With perfect security and flawless execution of procedures network breaches can be avoided. This paper comprises of the survey on detection methodology against clone attacks in WSN and the stages in methodology on various existing detection techniques and the survey chart is as shown in Figure 1. This paper is organized as follows: Section 2 presents network security trinity. Various attacks in WSN are discussed in Section 3 followed by the node based active attacks WSN in Section 4. In Section 5, stages of detection algorithm and literature review on various existing clone detection techniques are discussed. In section 6, security primitives and evaluation metrics for clone detection techniques were explained. The research challenges and issues depicted in section 7 and in the last Section 8, conclusion are described.

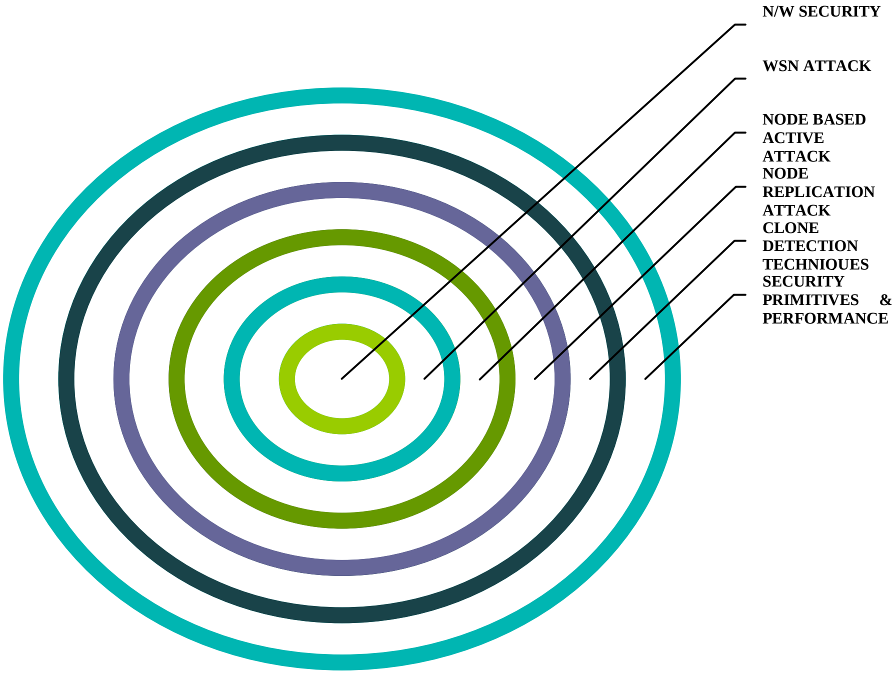

Figure 1. Survey chart or map of Existing Techniques

II. NETWORK SECURITY TRINITY

Network architecture succeeds in protecting the network can only by proper planning. Proper planning before an attack will greatly reduce the risks and increase the capabilities of a timely and effective detection and response if an attack occurs. The major three aspects in network security are detection, prevention and response. These are the network security trinity as shown in Figure. 2.

A. Detection

The attack to be identified in proper time and this process is called detection. Detection of a system compromise is tremendously critical. The mainly vital element of detection strategy is timely detection and notification of a compromise. To detect the intrusion, generally three types of detection methods are used. They are (i) Signature-based (ii) Statistical anomaly-based (iii) Stateful protocol analysis. The *signature-based detection methods* check packets and compares with pre- organized and pre- resolved attack patterns known as signatures. *Statistical anomaly-based detection method* have normal activity like information about what bandwidth, protocols, ports and devices connected to each other are used, and also the information about the port and devices which is to be used is generally connected to each other, then alert the user when anomalous traffic is detected. *Stateful protocol analysis detection method* that identifies variation of protocol states by comparing observed events with predetermined profiles of normally accepted definitions of benign activity [5].

B. Prevention

Prevention means taking steps to avoid damages quickly as possible before causing awful effect on a network. Network security researchers must continuously establish their capabilities by working smarter not harder. It is always better to prevent, then to track and act against. Cautious analysis and setting up is very essential requirement to be satisfied for preventing an incident. Intrusion prevention systems can be mainly classified into four different types. They are

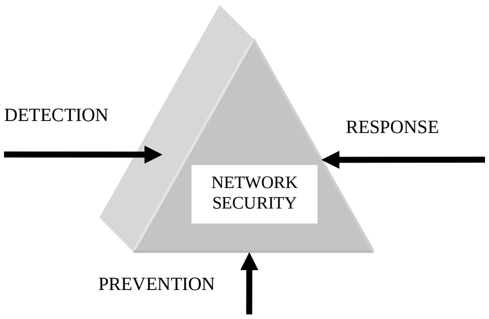

Figure 2. The Network Security Trinity

1. Network-based Intrusion Prevention System (NIPS): monitors the entire network by analyzing protocol activity for cautious traffic.
2. Wireless Intrusion Prevention Systems (WIPS): for suspicious traffic the wireless network is monitored by analyzing wireless networking protocols.
3. Network Behavior Analysis (NBA): checks network traffic to identify threats that generate odd traffic stream, such as Distributed Denial of Service (DDoS) attacks, definite forms of malware and policy breaches.
4. Host-based intrusion prevention system (HIPS): monitors a single host for doubtful activity by analyzing events happening within that host using a set up software package.

C. Response

Taking effective steps at appropriate time after a detection of attack in a network is said to be response. At present it is not a matter of ‘if’ a network system will be breached, but it is unavoidable to find out “when” and “by how much”. Networking can limit the effect of breach and restrain the revelation; but this means having the capacity to react once the initial event has been detected. A perceptive of the complete attack chain and all of its gears is vital in order to recognize the scope of the breach and possibly exposed responsive data. A network system may hope to scratch off the trespasser’s connection, exterminate the cause of the occurrence and recover the effected system. This method would be more practical when mission critical machines are affected and timely resurgence is precedence. For the detection process to have any cost there must be a sensible response, there are two response mechanisms. They are passive Intrusion Detection System (IDS) and active IDS. In passive, usually it works on off-line to analyze system log files and network traffic traces. In some cases, they also operate online to monitor host audit data and network traffic passively. Since it is unfeasible to present a highly resourceful way of reacting to high speed threats manually, automated response is proposed. On the other hand, active IDSs work on the fly and can launch immediate reactive or proactive responses to the attackers, automatically. Traditionally, the active response can be divided into two categories, such as reactive response and proactive response. Reactive responses are activated and executed after intrusions have been detected. Proactive responses refer to a set of preemptive actions to prevent an intended attack. The effectiveness of proactive responses is very much dependent on the capacity of the system to predict the attacks or the breaches.

III. ATTACKS IN WIRELESS SENSOR NETWORKS

This paper involves the basic steps on attacks in wireless sensor network as shown in Figure. 3 that concentrates on active and passive types [6]. The unofficial attacker monitors, take note and alter the data stream in the communication channel which is known as active attack. Active attacks encompasses of routing attacks in sensor networks, Denial of Service (DOS) attacks, fabrication, lack of cooperation, modification, impersonation and eavesdropping. The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. The Attacks against privacy is passive in nature. It comprises of monitor and eavesdropping, traffic analysis and camouflage adversaries.

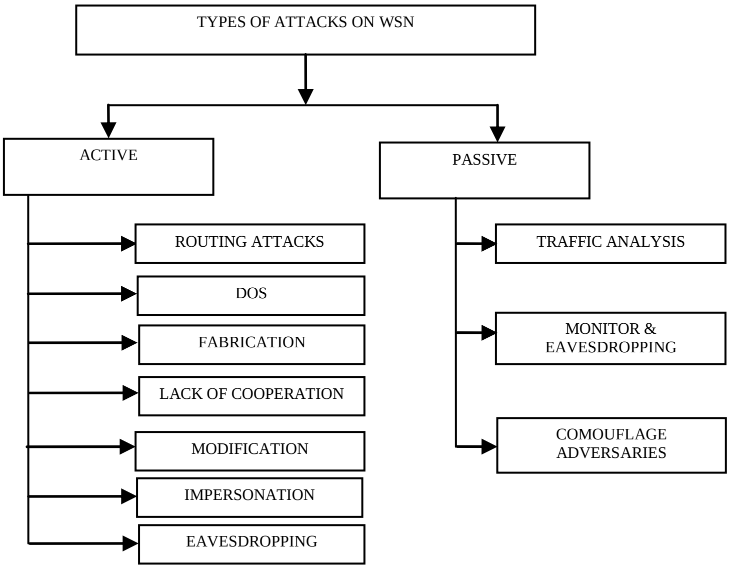

Figure 3. Types of Attacks in WSN Based on Active/Passive

A. Node Based Attacks In Wireless Sensor Networks

1. Types of Methods Under Node Based Active Attacks

A profound analysis on attack gives a deep study as shown in Figure. 4. It initially classifies as routing, modification, lack of cooperation, impersonation, fabrication. Routing is essential in WSN, but problem in routing is due to the rapid changes in the topology of the nodes and the devices. There are two types of routing, proactive and reactive. The routing attack can be done on lookup routing, routing updates and routing network partition. Modification attack is an attack in which an intruder shot to make changes to data on the target. In lack of cooperation type, it creates problem in cooperating with the network in all necessary activities. In impersonation attack type, the adversary or intruder pretense or imitate to be like an existing node in the network and causes the injection of malicious data or copies the node identity (ID) of an existing sensor node and pretend like an existing and can severely disrupt a performance of sensor network. In the fabrication attack, malicious node generates the incorrect information about the route between devices and thus creates false routing message.

From all of the above active types, specifically routing, modification, lack of cooperation, impersonation and fabrication comes under node based attacks [7]. The sink holes, Sybil attacks and selective forwarding attacks move towards *routing attack type*. Traffic attraction to a specific node through a compromised node is called sink hole attack. And so other nodes due to traffic attraction will be attracted by this attacker node and selects this path instead of choosing currently regularized path. In Sybil attack, a single node replicates itself and is accessible in the multiple locations. It means a single node makes multiple identifiers to other nodes in the network. In selective forwarding attack, the node refuses to forward packets and thus neighbours starts to use a new route. The physical attack comes under the *modification type of attack*. Highly at risk the hostile sensor environment that affects cryptographic secrets, tamper circuit and alters programming in sensors. This type of attack is called physical attack.

The node outage comes under *lack of cooperation attack type*. When the node stops its function such as reading, gathering and launching, then this attack is said to be node outage. It stops the functionality of WSN components physically or logically in the network. The false node and node replication attacks are grouped under impersonation attack type. In a false node attack, a node that have been added newly by an attacker and damage or takes into control the whole network. In node replication attack, a new node is added into the network by copying or clones the existing node ID. And thus severely interrupt a sensor network's performance by inserting the replicated nodes and easily manipulate or control the part of the network. In node subversion attack, capture of a node expose the leakage of cryptographic keys and thus compromise the full network. In node malfunction attack, a malfunctioning node that generates inaccurate data that affects integrity of sensor network especially for data-aggregating node. These node subversion and node malfunction attacks comes under *fabrication attack type*.

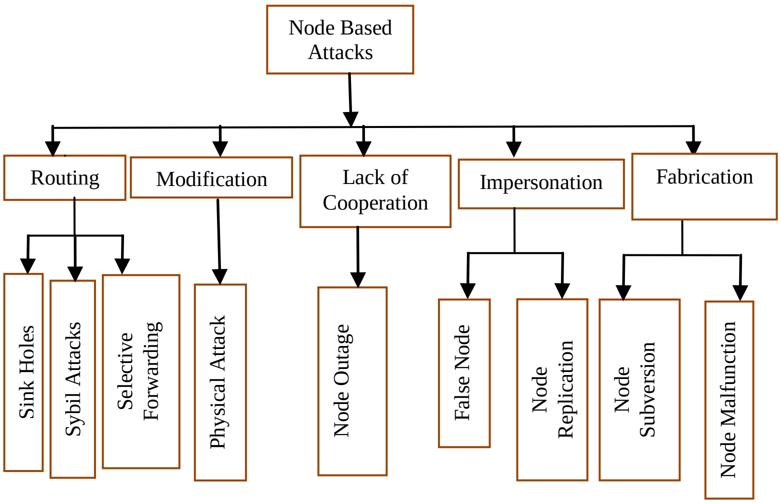

Figure 4. Types of methods under node based attacks in WSN

2. Node Replication Attack

We concentrate on node based attack in WSN network and focus on impersonation that deals with node replication attack. Node replication attack is also known as clone attack. In clone attack, a sensor node is confined by an intruder and the information is copied into its own sensors. Then it cleverly deploys the clones in the decided places. Node replication is ultimately detected by the node (called witness) on the intersection of two paths that begin from different network positions by the same node ID. Several attacks made using cloned nodes are exposed by many researches. In network, leakage of information is possible by cloned node. The adversary can also inject false information, or modify data passing all the way through the cloned nodes. It is not possible to regularly monitor nodes to detect potential tampering. Therefore, real time cloned detection is compulsory to combat these attacks.

The following three characteristics of a network are considered for a clone attack. Firstly, in terms of deterministic, the witnesses of a node are fixed in each execution. The adversary can easily compromises the nodes and deploy number of replicas if any protocols are deterministic. So it will be vulnerable to clone attacks. The deterministic scheme loses its resiliency. Secondly, in terms of non-resistance to smart attack, a smart adversary finds out and puts out of action only the critical witness nodes.

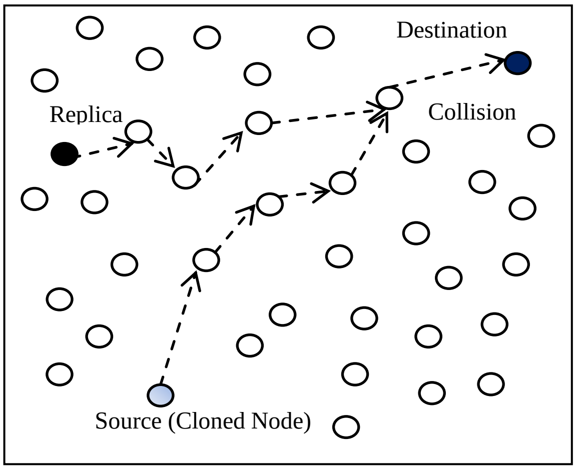

Figure 5. Clone Attack in Wireless Sensor Network

Critical witness nodes are the nodes that contain more information about the sensor nodes in the network and if the adversary captures these witness nodes then the network will be moved on critical state. And thirdly, need central control: If a centralized architecture is used in a sensor network and central node fails, then the entire network will subside; However, the reliability of the sensor network will be lessen and owe performance in data collection [8]. Figure 5 shows the clone attack scenario in wireless sensor network. Many wireless sensor nodes are available in a network. There occurs a source node, replicated node, collision occurring node and a destination node. In the presence of a clone attack, two nodes have same destination address. The possibility of occurrence of collision is very high. Most of the time collision occurs while reaching the destination.

B. Detection Algorithm against Clone Attack in WSN

1. Stages of Detection Algorithm

The existing papers on detection against clone attacks make only few differences in their techniques and remaining algorithms will be close to others. The common stages in this detection protocols involve node registration, key establishment, path selection and forwarding, detection techniques used, clone attack detection and revoke & response stages. In node registration stage, node is registered with identity id considering its location. The next stage is key establishment which is used for authentication purpose. In this key establishment stage each node creates its own key pair for secure to preserve authentication with digital signature. In path selection and forwarding stage, it deals with key distribution, shared key discovery and path-key establishment, path selection and packet forwarding. Next stage illustrates the various detection schemes or techniques used. The pre-final stage carries clone attack detection that identifies the clone attack. Finally, the revoke and response stage make a possible and immediate action to revoke the attack in a given network and gives better response.

A solid clone detection algorithm must be robust and fault tolerance. Initially node is registered. Each node to be broadcast its signed location claim to its neighbour which is a very necessary part of this protocol for detection. For indicating the authenticity of a digital message or documents, a mathematical scheme called a digital signature is used. It is necessary for authenticity of a digital message to be broadcast in a network. And thus it uses the signed authentication techniques. And an important design consideration for security protocols is based on key distribution between the nodes in the network. By using various path selection techniques, the packets are forwarded to the proper node. After using various detection protocols and if clone attack is detected then it goes for revoke and response phase. These are commonly used stages of detection methodology against clone attack in WSN as shown in Figure 6.

C. Clone Detection Techniques

The slight variations in between the existing detection methodology on clone attack detection are briefly explained below.

1. Deterministic Multicast (DM)

In DM, when a node broadcast its location claim, its neighbours forward that claim to a subset of the nodes called witnesses. Nodes location claim with limited subset of deterministically chosen “witness” nodes [2].Witnesses are chosen as a function of the node’s identity. If adversary replicates a node, the witnesses will receive two different location claims with similar node ID. i.e., conflicts location claims.

2. Bloom Filter

A counting Bloom filter is constructed for each node from the keys and issued for communication and to append a nonce. The bloom filter and nonce are encrypted with the particular node’s public key and forwarded to the exact node. Now that node decrypts messages and the number of times or the count of each key used is calculated and when it exceeds the threshold value, then the network is sure of with clone attack [9]. It uses gossip protocol to broadcast and it uses binomial distribution. It quantifies the extent of false positive and false negative in clone detection process.

3. SET: Clone Detection in Sensor Networks

This protocol proposed a work on a sensor network modelled as a set of non-overlapping sub region [10]. All nodes in the network have unique identifier. Sensor nodes in each sub-region form an exclusive subset. Since node identifier is unique, intersection of any two subsets should be empty. The intersection of subsets including these replicated nodes will not be empty when an adversary replicates the nodes, hence clone attack is detected. It first forms exclusive unit subsets among one-hop neighbours in the network in a distributed way. Secondly, it employs a tree structure to computer non-overlapped set operations and integrates interleaved authentication to prevent unauthorized falsification of subset information during forwarding.

4. Randomized Efficient Distribution (RED)

In RED protocol [11], the witness nodes' locations are determined by the claimer node ID and the seed rand. Random value (RAND) is shared among all the nodes. It is performed by distributed leader election. A trusted entity broadcasts a seed to the whole network in each detect iteration. The attacker cannot anticipate the witness nodes because the seed changes in every detect iteration. As described above, each neighbour node of a claimer node with probability becomes reporter node and forwards the claim message to witness nodes. The larger probability is the higher the success detect rate is and a claimer node tends to have more reporter nodes.

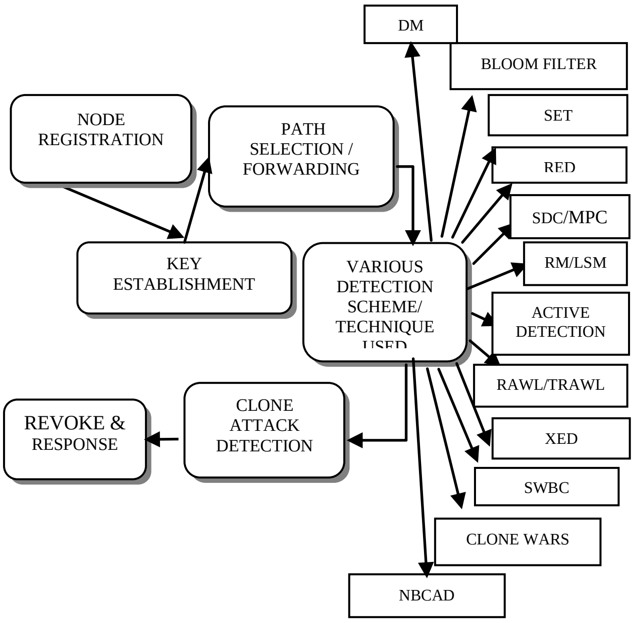

Figure 6. Stages of Detection Algorithm/ Methodologies against Clone Attack In WSN

5. Single Deterministic Cell (SDC) and Parallel Multiple Probabilistic Cells (P-MPC)

Two distributed replication detect protocols SDC and P-MPC was proposed in Zhu et al., 2007 [12]. The network is considered to be a geographic grid. Uniquely and randomly map a node's identity to one of the grid cells using a geographic hash function in the SDC protocol. To the mapping cell, the location claim message is forwarded. The location claim is flooded within the cell if the first copy of the location claim arrives at the destination cell. The nodes in the cell randomly become witness nodes. A node's identity is mapped to several cells in the grid increase the reliability to a large amount of replication nodes in P-MPC.. So, the candidate witness nodes for one node are nodes of several cells. Smart attacker can predict and subvert the witnesses with the predefined locations or cells.

6. Randomized Multicast (RM)/ Line Selected Multicast (LSM)

In RM, a particular node's neighbours send a copy of location claims to a set of randomly selected witness nodes. Birthday paradox predicts at least one collision with high probability. In LSM, rumour routing for location claim travels from one node to another node and it passes through intermediate node. It stores location claim and draws a line across the network [2]. If conflicting location claim never crosses the line, then the node at intersection will detect clone attack.

7. Active Detection

Active detection scheme is a fully distributed scheme. The given nodes are randomly chosen in the network. Each node checks the random nodes actively whether replicated or not. The two differing claims will be obtained by the querier if two replicas exist. The performance varies according to the witnesses chosen [4]. Here, the protocol uses relays to test whether randomly chosen nodes are replicated.

8. Random WaLk (RAWL)/Table Assisted RAndom WaLk (TRAWL)

Each of node’s neighbours probabilistically put ahead the claim to some nodes which is randomly selected and then the selected nodes send a message having the claim to make a start of random walk. And passed selected nodes are considered as witness nodes and will store the claim. The claims contain location and id of a node. When any witness receives the claim as different location with similar node id, then it is cloned node and thus the network should carry on the revoke process immediately [8]. TRAWL is based on RAWL with addition of trace table that uses claim digest to reduce memory and communication

9. eXtremely Efficient Detection (XED)

In XED, if two sensor nodes within the communication range of each other, it first generates Random (Rnd) number. Then exchange their Rnd number. It checks the received Rnd number whether already met. If it meets then there is a possibility of replicas to be detected. Location information is essential for all nodes if the witness finding strategy is applied [13].

10. Security in Wireless Sensor Networks by broadcasting location Claim (SWBC)

In SWBC, network is integrated with root node with its neighbouring nodes. Root node selection is the node which has maximum number of neighbouring nodes. Each root node and neighbouring node has their witness node and intermediate node to store up their location claims. By containing their own location they will shift their location to their root node. So the root node will make different on the sub-nodes and the adversary nodes [14].

11. History Information-Exchange Protocol/ History Information-Exchange Optimized Protocol (HIP/HOP)

In HIP, each node compares its own log with logs inward from its neighbors. However, in HOP, each node also compares the received logs between them, but not with the history log it owns [15]. Comparing history logs with direct neighbors only requires one-hop communications. The network has clone attack and goes for revoke process when an incompatible pair of locations is detected for a node. Each sensor records id and location of met neighbour and compares its own record with the one of met neighbour. They leverage the same level of collaboration between nodes, but exhibit a different level of meticulousness in order to detect the clone attack.

12. Neighbour Based Clone Attack Detection (NBCAD)

The NBCAD protocol uses public key cryptography to construct a linkage between sensor nodes and cluster after allocating of cluster head for each cluster [16]. And for secure communication, each node requests a session key from their cluster head. In a separate table it stores neighbor nodes location information and with the help of that table the finger print is computed. Each cluster head that receives the forwarded message also receives the finger print along with it and if it matches the existing information when compared with cluster head, then it recognizes the cloned node in the network.

IV. SECURITY PRIMITIVES AND EVALUATION METRICS FOR CLONE ATTACK DETECTION TECHNQUES

Each and every protocols performance may vary according to some primitives. The various detection techniques differ based on the security primitives such as cryptography, key distribution, node based, resilient, topology, routing, probability, witness based etc. that are considered in the respective techniques. Figure. 7 depicts the possible security primitives.

For the performance analysis and evaluation of replica detection protocols, four fundamental evaluation metrics are frequently used by the detection schemes. These are communication cost, memory cost, detection probability and detection time. Communication cost is defined as the average number of message sent by a sensor node while propagating the location claims. Memory cost defines the average number of the location claims store up in a sensor node. Detection probability is an significant evaluation metric which shows how accurately a protocol can recognize and detect the clones or replicas. The detection time is basically the delay between actual replica node deployment and detection.

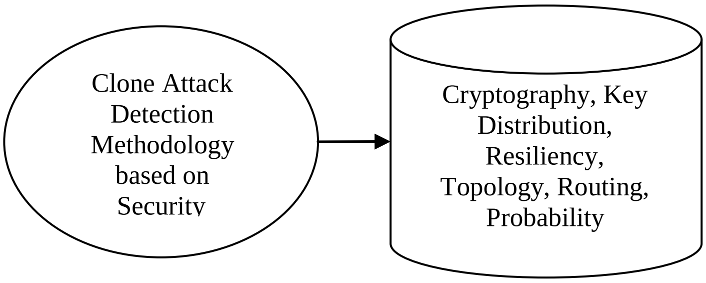
Clone Attack Detection Methodology based on Security
Cryptography, Key Distribution, Resiliency, Topology, Routing, Probability

Figure 7. Security primitives commonly used for clone attack detection techniques

- **Cryptography** is a technique that combines words with images and to hide information in storage or transit. It is normally related with scrambling plaintext. The ordinary text ie., the clear text converted into cipher text which is said to be encryption and back again into original text is decryption. It is the technique that puts up and analyzes protocols that thwart third parties or the public from reading private messages. Data confidentiality, data integrity, authentication, and non-repudiation are the choice of aspects in information security for central to modern cryptography.
- **Key distribution** is an important concern in WSN design. Due to memory and power constraints, it is necessary to be well arranged to construct a fully functional network. Before deployment, the method of key distribution onto nodes is termed as key predistribution. When it reaches its target position, the nodes build up the network using their secret keys after deployment. Key distribution, shared key discovery and path-key establishment are the phases basically come under key predistribution scheme. The aspects on key predistribution schemes involve local and global connectivity, and resiliency. Local connectivity refers the probability that any two sensor nodes have a common key with which a secure link established for communication. The fraction of nodes that are key connected graph over the number of all nodes is global connectivity.
- **Resiliency** the keys in number of nodes are compromised since the number of links that cannot be compromised. So it is fundamentally the quality of resistance in opponent to the attempts to hack the network. Computational cost is the quantity of computation done during these phases. Hardware cost is usually the rate of the memory and battery in each node.
- **Topology** a specific mathematical idea central to the area of mathematics is termed as topology. In a relaxed way, a topology gives the information about how the elements of a set relate spatially to each other. The different topologies may be in same set and it may be real line, the complex plane or the Cantor set. Topology developed as a ground of study out of geometry and set theory throughout analysis of such concepts as space, dimension, and transformation. Topology is a structure that characterizes as a topological space by taking proper care of properties such as convergence, connectedness and continuity, in the lead transformation.
- **Routing** is the process of selecting best paths in a network. In the past, the term routing also meant forwarding network traffic among networks. It mainly concern with selecting of best paths in a network. Routing in networking concerned primarily with routing in electronic data networks using packet switching technology. In packet switching networks, routing directs packet forwarding through intermediate nodes. Intermediate nodes are classically network hardware devices such as routers, bridges, gateways, firewalls, or switches. General-purpose computers can also forward packets and perform routing, though they are not specialized hardware and may suffer from limited performance. The routes record to various network destinations is maintained on routing process normally that directs forwarding on the basis of routing tables. So it is very important for efficient routing for constructing routing tables. More often routing algorithm can use single network path at a time and multi path routing enables multi alternative paths.
- **Probability Distribution** assigns a probability to each measurable subset of the possible outcomes of a random experiment, survey, or procedure of statistical inference. A probability distribution can either be univariate or multivariate. A univariate distribution gives the probabilities of a single random variable taking on various alternative values that includes binomial distribution, the hyper geometric distribution, and the normal distribution and a multivariate distribution is a joint probability distribution that gives the probabilities

of a random vector and the multivariate normal distribution is a commonly encountered multivariate distribution.

- **Witness Method** In a distributed detection, each node broadcast its claim that carries identity and location information of a node to its neighbor. Then the node's claim will be sent by the neighbor to a selected node called a witness node. The intermediate nodes forwarding location claims can also be witness nodes besides of selected nodes. The node replication attack was detected by witness node by checking the ID with its location. If replicated nodes present in the network then at least one witness node is possible to receive conflicting location claims according to birthday paradox. The appropriate actions to revoke the node's credentials should be taken when replica is detected in the network.

Table I. Performance Analysis of Different Protocols

Sl. No	Protocols	Resiliency	Communication Cost	Memory Cost
1.	LSM	×	O(√n)	O(√n)
2.	RED	×	O(√n)	O(1)
3.	SDC	✓	O(√n)	O(1)
4.	RAWL	✓	O(√n log n)	O(√n log n)
5.	TRAWL	✓	O(√n log n)	O(1)^{2}

'n' is the number nodes in the network

- **Signature Based** A mathematical scheme for signifying the legitimacy of a digital message or documents is digital signature. A digital signature scheme classically consists of three algorithms. They are key generation, signing and signature verifying. There are various reasons to sign such a hash or message digest as a substitute of the whole document. For efficiency, the signature is much shorter and thus time consumes and hashing is usually much faster than signing execution. Messages are naturally bit strings in case of compatibility, but some signature based scheme constrain on other domain such as, in the case of Rivest-Shamir-Adleman (RSA), number modulo a composite number. A hash function can be used to convert a subjective input into the proper format. For integrity, the text without hash function which is to be signed may have to be separated in blocks small enough for the signature scheme to take steps on them directly. However, the receiver of the signed blocks is not able to distinguish if all the blocks are present and in the proper order. In clone attack detection, the researcher should select an algorithm that is suitable for their detection in terms of communication, computational and memory cost. . In table 1, we show the cost comparison of communication and memory of different protocols and its resiliency.

V. Research Issues and Challenges

Detection is a tremendously important problem with direct application in various domains. A key observation is that performance of existing is not upto satisfactory level. It needs much refinement in the nature of witness selection, the nature of detection probability, the nature of key based technique, the constraints and the assumptions.

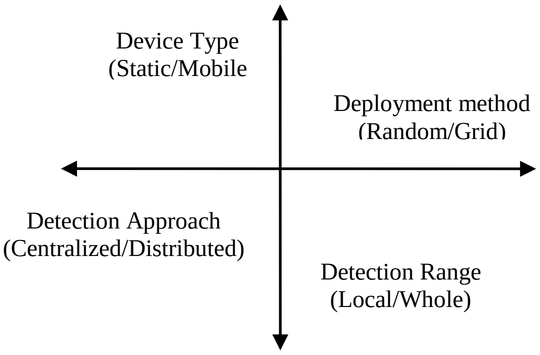

Figure 8. Classification of Selection Criteria

Selection of primitives related to detection methodology will augment the performance of clone attack detection. Choosing the perfect set of security requirements and constraints will give rise to an efficient detection against clone attack.

Based on our review, we observe that the detection technique can be made more efficient by choosing any one of the relevant selection criteria namely device type, deployment method, detection method and detection range as shown in Figure 8. In static device type, the sensor nodes are stationary or static; that is, the sensor nodes are deployed randomly, and their positions do not change after deployment. On the other hand in mobile device type, the sensor nodes can move on their own, and they can interact after deployment with the physical environment by controlling their own movement. The centralized detection approach each node has a control on base station or central control. In distributed detection approach, each node had its own control and there is no need of central control. In deployment method, the sensor nodes can be either randomly distributed or distributed according to grid wise. The detection range involves locally or on the whole of the network. The respective selection criteria for some of the protocols are depicted in table II.

Table II. Selection Criteria of different protocols

Sl.No.	Protocols	Device type (Static/Mobile)	Detection Approach (Centralized/ Distributed)	Deployment method (Random/Grid)	Detection range (Local/Whole)
1.	LSM	Static	Distributed	Random	Whole
2.	RED				
3.	SDC				
4.	RAWL				
5.	TRAWL				

Table III. Review summary of Node Replication Detection Techniques

Sl. No.	Reference No./ Author/Year	Protocols	Performance Analysis	Methodology Primitive Used
1.	B. Parno et al., 2005, [2]	DM	Communication cost improved by selecting a fixed set of witnesses	Witness based Detection Probability
2.	R. Brooks et al., 2007, [9]	BLOOM FILTER	It quantifies the extent of false positives and negatives in the clone detection process. It plots the maximum component size of the network versus false positive rate for both grid and adhoc networks.	Key based
3.	H. Choi et al., 2007, [10]	SET	More efficient in terms of communication and memory cost. Support a reliable and secure detection of clone attack. Probabilistic analysis shows high resiliency and low transmission overhead.	Base station based, Detection Probability
4.	R. Pietro et al., 2007, [11]	RED	Highly efficient in terms of communication, memory and computation. It is ID/Area oblivious and so, improvement in detection capability.	Witness based Detection Probability
5.	B. Zhu et al., 2010, [12]	SDC/P-MPC	Communication and memory cost. Achieve high probability of detection.	Witness based Resiliency
6.	B. Parno et al., 2005, [2]	RM/LSM	Tend to be more space efficient. Storage requirement reduced by using time synchronization enhancement.	Witness based Resiliency Detection probability

Sl. No.	Reference No./ Author/Year	Protocols	Performance Analysis	Methodology Primitive Used
7.	C.A. Melchor et al., 2009, [4]	ACTIVE DETECTION	Reduces number of witness nodes. It has constant number of scrutinized nodes per node. And thus memory usage per node reduced. No need of choosing a clever distribution of the relays and thus communication overhead also reduced. Increases detection rates.	Detection Probability Witness based
8.	Zeng et al., 2010, [8]	RAWL/ TRAWL	Less Communication cost due to t-step random walk. Less Memory cost due to claim digest. High probability detection due to torus structure. Better security properties.	Witness based Detection Probability Signature based
9.	C.M. Yu et al., 2008, [13]	XED	Constant communication is only required. Memory cost reduced because no need of location information of sensor nodes.	Witness based Detection Probability Time based
10.	S. Meenatchi et al., 2014, [14]	SWBC	Communication overhead is reduced. Detection probability in terms of iteration is high.	Witness based Detection Probability
11.	M. Conti et al., 2013, [15]	CLONE WARS	High Detection rate. Communication cost is reduced.	Detection rate Detection Probability
12.	J. Anthoniraj and Dr. T. Abdul Razak, 2015, [16]	NBCAD	Reduce the transmission range and power consumption of the nodes Less memory space. High Detection ratio and higher probability.	Cluster based Detection Probability Resilient

The major issues in clone attack detection scheme are as follows:

1. Probably when detection rate increases the computation cost also increases.
2. On observation, computation cost will be decreased if less number of witness nodes is used.
3. Almost certainly communication cost depends on the selection of witness nodes.
4. High probability detection is possible based on topology.
5. Clever distribution of witness path may reduce communication overhead.
6. Normally probabilistic analysis shows high resiliency.
7. Node mobility is more challenging for energy conservation in computing.
8. Grid based deployment will be more efficient in case of reachability and computational cost.
9. On network consideration, local detection rather than whole area detection will be minimum time consumption and less complicated.
10. On our study, distributed detection outperforms clone attack detection in WSN.

VI. Conclusion

This paper is better organized for the research community mainly on network security. The WSN deployed in hostile atmosphere are susceptible to clone attacks. WSN are employed for some critical application, so one of the primary concerns of this type of system should be considered as its security. In network security, prevention, detection and response are the three main aspects of network security trinity. The mainly essential element of these trinity strategy is time based which made the network to be secured or critical. In this paper, various attacks possible in WSN are listed with a special emphasis to node based attacks and also summarised clone attack detection technique. The existing detection algorithms against clone attacks are detailed and the performance of different methods are analysed with a neat tabulation. We look into necessary security primitives so as to reveal their respective contribution. The discussed security primitives play a vital role in the performance of detection techniques. A selection of proper combination on the discussed selection criteria finds immense use in clone detection technique. The detection technique is the major issue in security. This paper will be benefited and widely routed to the researches for new challenges and emerging trends on various detection methodologies against clone attack. The various detection methodologies against clone attack will be excellent in security, with suitable selection criteria and detection primitives.

REFERENCES

[1] Akyildiz, I. F., W. Su, Y. Sankarasubramaniam, and E. Cayirci, Wireless Sensor Networks: A Survey Computer Networks, pp.393-422, 2002.

[2] Parno, Bryan, Adrian Perrig, and Virgil Gligor, Distributed detection of node replication attacks in sensor networks, Security and Privacy, IEEE Symposium, pp.49-63, 2005.

[3] Bonaci, Tamara, Linda Bushnell, and Radha Poovendran, Node capture attacks in wireless sensor networks: a system theoretic approach, Decision and Control (CDC) 49th IEEE Conference, pp.6765-6772, 2010.

[4] Melchor, Carlos Aguilar, Boussad Ait-salem, and Karim Tamine, Active detection of node replication attacks, International Journal of Computer Science and Network Security (IJCSNS), No.9, pp.13–21, 2009.

[5] Rimbert M. Rivera, Global Information Assurance Certification Paper, GISO Practical Assignment, Vol.1.1, pp.1-28, 2002.

[6] Santhosh S., Radha R., A Novel Security Model For Preventing Passive and Active Attacks in WSNs, International Journal of Advanced Research in Computer and Communication Engineering ,Vol.2, No.10, pp.3813-3816, 2013.

[7] Padmavathi, Dr G., and Mrs Shanmugapriya, A survey of attacks, security mechanisms and challenges in wireless sensor networks, 2009.

[8] Zeng, Yingpei, Jiannong Cao, Shigeng Zhang, Shanqing Guo, and Li Xie, Random-walk based approach to detect clone attacks in wireless sensor networks, Selected Areas in Communications, IEEE Journal, Vol.28, No.5, pp.677-691, 2010.

[9] Brooks, Richard, P. Y. Govindaraju, Matthew Pirretti, Narayanan Vijaykrishnan, and Mahmut T. Kandemir, On the detection of clones in sensor networks using random key predistribution, Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions, Vol.37, No.6, pp.1246-1258, 2007.

[10] Choi, Heesook, Sencun Zhu, and Thomas F. La Porta, SET: Detecting node clones in sensor networks, In Security and Privacy in Communications Networks and the Workshops, Secure Comm Third International Conference IEEE, pp.341-350, 2007.

[11] Conti, Mauro, Roberto Di Pietro, Luigi Vincenzo Mancini, and Alessandro Mei, A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks, Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing, pp. 80-89, 2007.

[12] Zhu, Bo, Sanjeev Setia, Sushil Jajodia, Sankardas Roy, and Lingyu Wang, Localized multicast: efficient and distributed replica detection in large-scale sensor networks, Mobile Computing, IEEE Transactions Vol.9, No.7, pp.913-926, 2010.

[13] Yu, Chia-Mu, Chun-Shien Lu, and Sy-Yen Kuo, Mobile sensor network resilient against node replication attacks, Sensor, Mesh and Ad Hoc Communications and Networks SECON'08, 5th Annual IEEE Communications Society Conference, pp.597-599, 2008.

[14] Meenatchi, S., C. Navaneethan, N. Sivakumar, P. Thanapal, and J. Prabhu, Swbc-Security In Wireless Sensor Networks By Broadcasting Location Claims, Journal of Theoretical and Applied Information Technology, Vol.64, No.1, pp.16-21, 2014.

[15] Conti, Mauro, Roberto Di Pietro, and Angelo Spognardi, Clone wars: Distributed detection of clone attacks in mobile WSNs, Journal of Computer and System Sciences, Vol.80, No.3, pp.654-669, 2014.

[16] Anthoniraj J., Dr. T. Abdul Razak, NBCAD: Neighbor Based Clone Attack Detection in Cluster Based Static Wireless Sensor Networks, In International of Engineering and Technology (IJET), Vol.7, No.3, pp.912-921, 2015.

[17] Yu, Chia-Mu, Chun-Shien Lu, and Sy-Yen Kuo. "Mobile sensor network resilient against node replication attacks." In Sensor, Mesh and Ad Hoc Communications and Networks, 2008. SECON'08. 5th Annual IEEE Communications Society Conference on, IEEE, pp.597-599, 2008.

[18] Zeng, Yingpei, Jiannong Cao, Shigeng Zhang, Shanqing Guo, and Li Xie. "Random-walk based approach to detect clone attacks in wireless sensor networks." Selected Areas in Communications, IEEE Journal on 28, no. 5, pp.677-691, 2010.

[19] Zhu, Bo, Sanjeev Setia, Sushil Jajodia, Sankardas Roy, and Lingyu Wang. "Localized multicast: efficient and distributed replica detection in large-scale sensor networks." Mobile Computing, IEEE Transactions on 9, no. 7, pp.913-926, 2010.