IJCSC 0973-7391 Vol 6 • Number 2 April - Sep 2015 pp. 316-323 **Impact Factor: 2.5** **Available at** www.csjournals.com

A Review: Detection of Clones in Wireless Sensor Network

Manisha R. Deore[1], R. V. Patil[2]
[1]Master Student Computer Science & Engineering, SSVPS'S B.S.Deore College of Engineering, India
[2]Assistant Professor, Computer Science & Engineering, SSVPS'S B.S.Deore College of Engineering, India
[1]deore.manisha28@gmail.com; [2] patil.rajedra@ssvps.com

Abstract: Now a days wireless sensor networks have number of applications in different variety of fields such as military applications, environmental monitoring, and collecting information from in hospitable areas. But due to the more use of sensor network the risk of data leakage is also more. And results of it affect the overall working of the network. Many types in the attacker node collect some nodes from the network and their information will be collected. Then some clones of the captured nodes will be created with same identity and they will be place into the network. These nodes act as original node of the network data and they will use all the privileges of the original captured nodes. So these types of the clones in the network should be detected before they can do much harmful to the network. Therefor several types of algorithms are developed for this purpose. Thus, in this paper we survey the major topics in wireless sensor network related to the security purpose, and present many of the current attacks from the network, and finally list their corresponding defensive measures.
Keywords: Wireless Sensor network, Clones, Attack, Detection methods.

I. INTRODUCTION

A wireless sensor network (WSN) consists of autonomous sensor nodes to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion. The most of networks are bi-directional, also that control the sensor activity. Today that type of networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. A sensor node is a tiny device that includes three basic components: a sensing subsystem for data acquisition from the physical surrounding environment, a processing subsystem for local data processing and storage, and a wireless communication subsystem for data transmission. In addition, it contain a power source supplies the energy needed by the device to perform the programmed task. This power source often consists of a battery with a limited energy budget. There are different Sensors such as pressure, accelerometer, camera, thermal, microphone, etc. They monitor conditions at different locations, such as temperature humidity, vehicular movement, lightning condition, pressure, soil makeup, noise levels, the presence or absence of certain kinds of objects mechanical stress levels on attached objects, the current characteristics such as speed, direction and size of an object. Normally a sensor node combines the abilities to compute, communicate and sense [1].

Advance developments in wireless communications of low-cost and low power wireless sensor networks are developed. WSNs have different number of applications and also have unique challenges. They are actually systems contain many small devices which is called sensor nodes, that monitoring different environments ; i.e. sensors cooperate to each other and collect their local data to reach a global view .Sensor nodes also can operate autonomously. In WSNs there are two other components, called "aggregation points" and "base stations", which have more powerful resources than normal sensors. Aggregation points collect information from their nearby sensors, integrate them and then forward to the base stations to process gathered data, as shown in figure1. Limitations such as cost, invisible deployment and variety application domains, lead to requiring small size and limited resources. Also, WSNs are responsible to many types of attacks such as physical attacks; these attacks are one of the most dangers and harmful on WSNs. Due to unsafe nature of communication channel, unsecure and broadcast media, and limited resources, also security techniques of networks are impossible in WSNs; therefore, security is a vital and complex requirement for these networks, especially against to the physical attacks [5].

II. SENSOR NODE ARCHITECTURE

A sensor node typically consists of five main parts: one or more sensors gather data from the environment. The central unit in the form of a microprocessor manages the tasks. A transceiver (included in the Figure 2) communicates with the environment and a memory is used to store temporary data or data generated during processing. The battery supplies all parts with energy (see Figure 2). To assure a sufficiently long network lifetime, energy efficiency in all parts of the network is crucial. Due to this need, data processing tasks are often spread over the network, i.e. nodes co-operate in transmitting data to the sinks. Although most sensors have a traditional battery there is some early stage research on the production of sensors without batteries, using similar technologies to passive RFID chips without batteries.

The development of sensor nodes is influenced by

- increasing device complexity on microchips,
- high performance, wireless networking technologies,
- a combination of digital signal processing and sensor data acquisition,
- advances in the development of micro electromechanical systems (MEMS), and
- Availability of high performance development tool s [5].

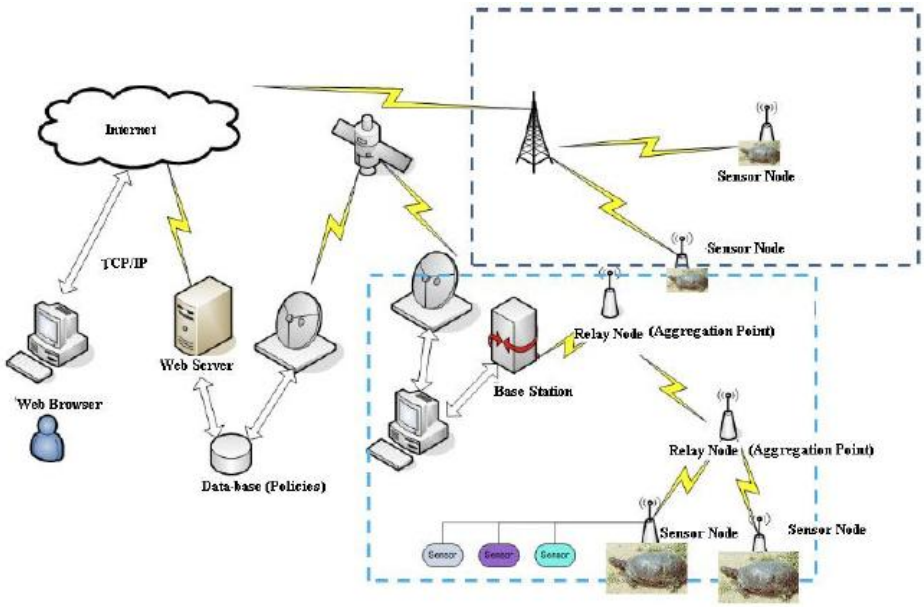

Fig. Error! No text of specified style in document.**: A simple wireless sensor network**

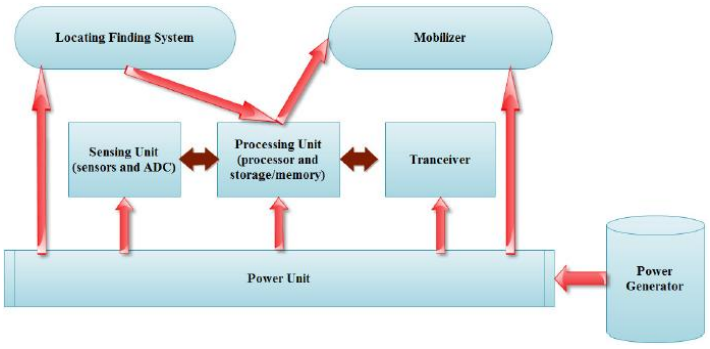

Fig. 2: Sensor Node Architecture [5]

III. CHARACTERISTICS OF WSN

- Power consumption constrains
- Node failures due to ability to cope
- Mobility of nodes
- Topology of network is Dynamic
- Lack of communication
- Heterogeneity of nodes
- Large scale of deployment
- Ease of use
- Unattended operation [5]

IV. FIELDS OF APPLICATIONS OF WSN

1.Security and Surveillance: Now a day`s wireless sensor networks can be an integral part of military command, control, communications, computing intelligence, surveillance, reconnaissance and targeting systems.

2. Environmental Monitoring: The term Environmental Sensor Networks has evolved to cover many applications of WSNs to earth science research. This includes sensing oceans, glaciers, forests, etc. Some other major areas are listed below

- Air pollution monitoring: Wireless sensor networks have been design for several cities to monitor the dangerous gases for citizens
- Forest fires detection: A network of Sensor Nodes can be installed in a forest to detect when and where fire has started. The nodes can be attached with sensors to measure temperature of fire, monitor gases which are produced by fires in the trees or vegetation; due to Wireless Sensor Networks, the fire brigade will be able to know when a fire is started and how it is spreading in environment.
- Landslide detection: This detection system makes use of a wireless sensor network to detect the movements of soil and also what are the changes in various parameters that may occur in landslide.

3. Health Applications: wireless Sensor networks are also mostly used in health care area. In many other cases some hospital sensor networks are developed to monitor patient physiological information, to control the track and monitor patients and doctors and inside a hospital. The idea of embedding wireless biomedical sensors inside human body is promising, although many additional challenges exist: the system must be ultra-safe and reliable require minimal maintenance; energy-harnessing from body heat.

4 Energy Control System: Societal-scale sensor network can greatly improve the efficiency of energy-provision chain, which consists of 3 components the energy-generation, distribution, and consumption infrastructure

5. Area monitoring: Another type of application of wireless sensor network is area monitoring which is a common application. In this area monitoring application, the WSN is deployed to some phenomenon is be monitored. An example is the oil pipelines.

6. Agriculture Applications: Agriculture Using wireless sensor networks within the agricultural industry is increasingly common; using a wireless network frees the farmer from the maintenance of wiring in a difficult environment Wireless sensor networks are also used to control the temperature and humidity levels inside commercial greenhouses.

7. Industrial applications: Wireless sensor networks have developed for machinery condition-based maintenance (CBM) that offer cost savings and also enable new functions.

8. Structural monitoring: This application of wireless sensors can be used to monitor the movement within the buildings and also infrastructure such as bridges, embankments, and tunnels etc.

V. ACTIVE ATTACKS AND THEIR CATEGORIES IN WSN

Wireless Sensor networks are easily fall to security attacks due to the broadcast nature of communication. Also wireless sensor networks have additionally in which nodes are often placed in a hostile environment where they are not protected from others. There are two types of attacks active attacks and passive attacks. Figure3 shows the classification of attacks and Figure 4 shows attacks classification on Wireless Sensor Network.

A. Passive Attacks

In this type of attack the monitoring and listening of the communication by unauthorized attackers are known as passive attack. The Attack which is against privacy is passive in nature .Attacks against Privacy. The main privacy problem is not that sensor networks enable the collection of information. In fact, much information from sensor networks could probably be collected through direct site surveillance. Rather, sensor networks intensify the privacy

problem because they make large volumes of information easily available through remote access. Monitor and Eavesdropping: This is the common type of attack to privacy. It easily discover the communication contents, by snooping to the data.
Traffic Analysis: Even when the messages transferred into the encrypted form , it still chances to a high possibility analysis of the patterns of the communication.

B. Active Attacks
In this type of attack the unauthorized attacker which monitor, listens to and modifies the data into the communication channel are known as active attack.
The following attacks are active attack
1. Routing Attacks in Sensor Networks
2. Denial of Service Attacks
3. Node Subversion
4.Node Malfunction
5.Node Outage
6.Physical Attacks
7.Message Corruption
8.False Node
9.Node Replication Attacks
10.Passive Information Gathering

1. Routing Attacks in Sensor Networks

the attacks which act on the network layer are called routing attacks. The following are the attacks that happen while routing the message.

a) Spoofed, altered and replayed routing information

an unprotected routing is vulnerable to these types of attacks, as every node acts as a router, and therefore it directly affect routing information in network. Such as Create routing loops, Extend or shorten service routes, Generate false error messages and also Increase end-to-end latency.

b) Selective Forwarding

In this selective forwarding attack malicious node can selectively drop only certain packets. Especially effective if combined with an attack that gathers much traffic via the node

c) Sinkhole Attack

Attracting traffic to a specific node in called sinkhole attack. In this attack, the adversary's goal is to attract nearly all the traffic from a
particular area through a node. This type of attack typically works by making a compromised node look attractive to surrounding nodes.

d) Sybil Attacks

A single node duplicates itself and presented in the multiple locations. The Sybil attack targets fault tolerant schemes such as distributed storage
multipath routing and topology maintenance. In a Sybil attack, a single node presents multiple identities to other nodes in the network

e) Wormholes Attacks

In the wormhole attack, an attacker records all packet at one location in the network, then tunnels them to another location, and retransmits them into the
network which is call as wormholes attack.

f) HELLO flood attacks

An attacker sends or replays a routing protocol's HELLO packets from one node to another node into the network with more energy. This attack uses HELLO packets as a one type of strong weapon to convince the sensors in WSN. In this type of attack an attacker with a high radio transmission range and power sends HELLO packets to a number of sensor nodes in Wireless Sensor Network.

2. Denial of Service

Denial of Service (DoS) is occurs due to the unintentional failure of nodes or malicious action of the node. In wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks can be jamming and tampering, DOS attack at link layer is collision, exhaustion and unfairness, at

network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by de synchronization.

3. Node Subversion
   Capture of a node may provide its information. In this type a particular sensor might be captured, and information data stored on it might be obtained
4. Node Malfunction
   In this type a malfunctioning node will generate inaccurate data that could expose the identity of sensor network especially when it is a data-aggregating node such as a cluster leader.
5. Node Outage
   Node outage is the situation that occurs when a node stops its function. In the case where a cluster leader stops functioning, the sensor network protocols should be robust enough to mitigate the effects of node outages by providing an alternate route.
6. Physical Attacks
7. Sensor networks typically operate in hostile environments. In such environments, the small form factors, combined with the unattended and distributed nature of their deployment make them highly susceptible to physical attacks, i.e., threats.
8. Message Corruption
   Any modification of the content of data by an attacker is message corruption
9. False Node
   A false node involves the addition of a node by an adversary and causes the injection of malicious data.

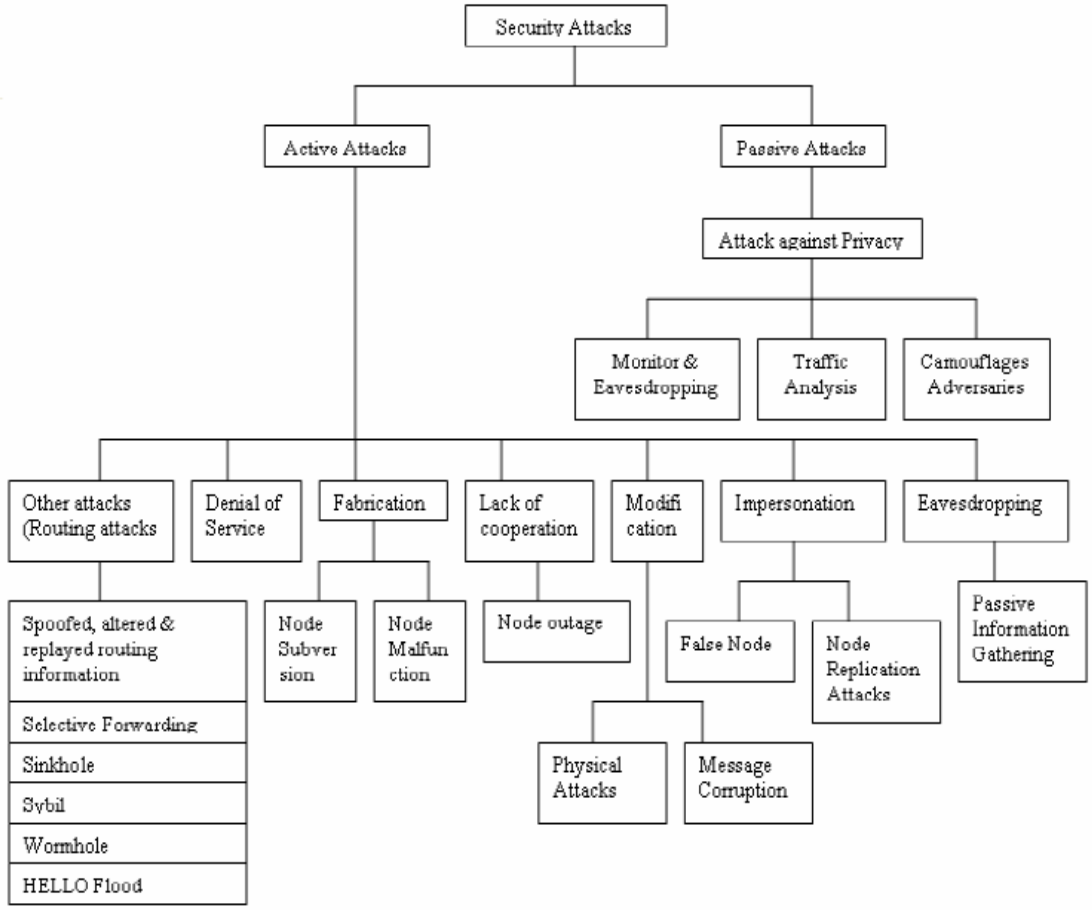

Fig. 3: Classification of Attacks in WSN

10. Node Replication Attacks
    Conceptually, a node replication attack is one type of simple attack ; an attacker to add a node into the network by copying the node ID of an existing sensor node. Packets can be corrupted or even misrouted. This can result in a disconnected network, false sensor readings, etc.

11. Passive Information Gathering
    An adversary with powerful resources can collect information from the sensor networks if it is not encrypted. An intruder with an appropriately powerful receiver and well-designed antenna can easily pick off the data stream. Interception of the messages containing the physical locations of sensor nodes allows an attacker to locate the nodes and destroy them. Besides the locations of sensor nodes, an adversary can observe the application specific content of messages including message IDs, timestamps and other fields. To minimize the threats of passive information gathering, strong encryption techniques needs to be used.

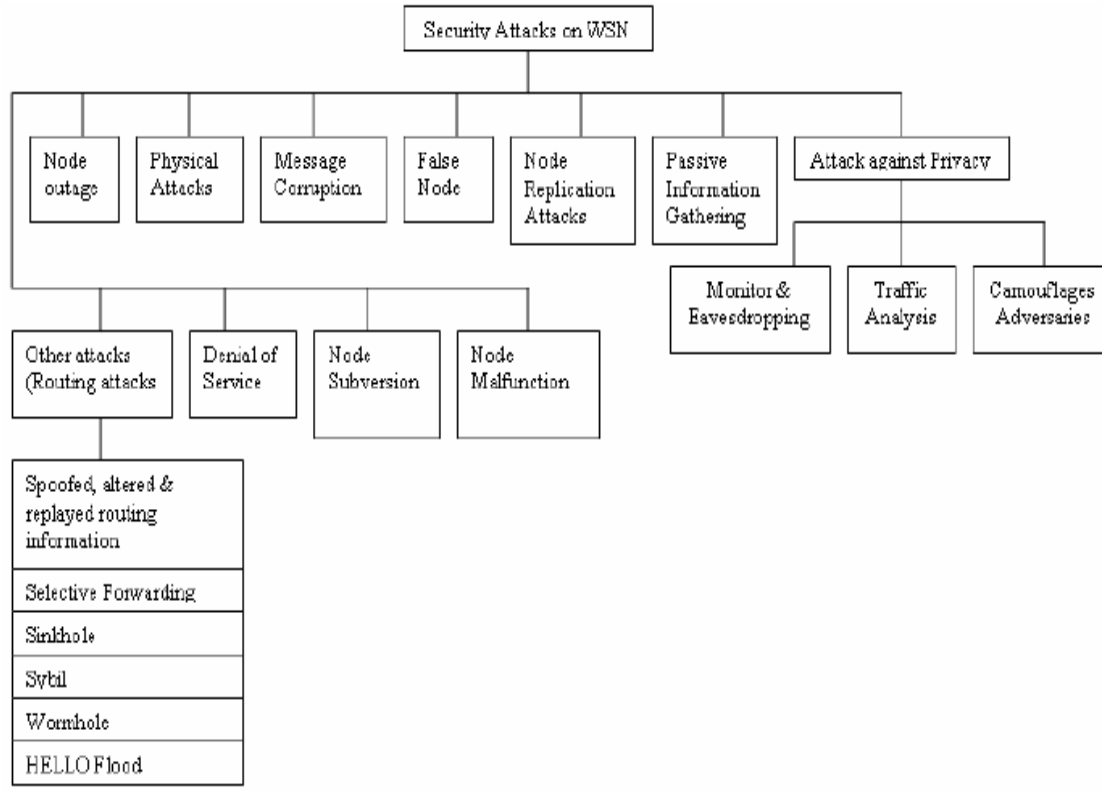

Fig. 4: Classification of Security Attacks in WSN

The active attacks affect different layers of the network. The classification of different attacks, their effects and also the layer in which it attacks are listed in Table1.

Table: 1 Category of Active Attacks

Attacks	Classification	Attack Layer	Attack Effects	Preventive Measures
Service Availability and Bandwidth Consumption Attacks	-Flooding Attack - Jamming Attack - Replay Attack - Selective Forwarding Attack	Transport - Physical - Network - Network	-Exhaustion of Resources -Transmission Interference, Exhaustion of resources -crash and exploit vulnerable holes in poorly designed system -Unfaithful routing information in the network	Client Puzzles Spread Spectrum techniques Priority messages Mapping Lower duty cycles Mode change Egress filtering Anti-replay protection Multiple Disjoint routing paths Diversity coding
Routing Attacks	-Unauthorized Routing Update Attack - Wormhole Attack - Spoofing Attack - Sinkhole Attack	Network	-Exploit Routing protocol -Launches different attacks -Network is complicated -Attracts the traffic by creating false routing - Causes Jamming in the network traffic	False routing information detection Probing Identity protection
Identity Attacks	-Impersonate Attack - Sybil Attack	Network	-Unauthorized access of server using victims credentials -Packets traversing by attacked channel is dropped	Radio Resource Testing Random Key Predistribution RSSI based detection scheme Code and Position verification
Data Integrity and Confidentiality Attacks	-Denial of Service Attack - Eavesdropping Attack - Node Replication Attack	- Physical, Data link, Network, Transport, Application -Network - Network	-Prevents the functioning of the network -Causes jamming and tampering of the network -Reduces data confidentiality -Controls the captured node and replicates, launches insider attacks	Hiding Access restriction

VI. DETECTION METHODS FOR CLONES IN WSN

Wireless Sensor Nodes is detected by various detection methods. The detection methods are classified as centralized and distributed detection and they are further classified as shown in Figure.5.

1. Centralized Detection Methods: In wireless sensor networks there is only one centralized detection method namely the Sequential Probability Ratio Test (SPRT).Sequential Probability Ratio Test (SPRT): In SPRT, each and every time the node claims its location and time information to their neighbors and they forward it to the base station when they enter into a new location. By taking speed as the sample the base station computes the SPRT and when the limit is exceeded it is detected as replica.
2. Distributed Detection Methods: The distributed detection methods [1] used in mobile wireless sensor networks are XED, EDD and mobility assisted distributed detection methods are the existing detection methods.

- Extremely Efficient Detection (XED): In XED, the sensor nodes communicate with each other through the random numbers which has been generated already. If they are unable to generate the random numbers they are detected as replicas.
- Efficient and Distributed Detection (EDD)
  In EDD, the two assumptions are
- Offline Step- In the network without replicas, the number of times a node meets a specific node should be limited for a given time interval
- Online Step- In the network with replicas, the number of times a node meets a particular node should be greater than the threshold.

A node is capable of detecting replicas should be able to differentiate between the above two steps.

- Mobility Assisted Distributed Detection

In this detection method, when two nodes meet each other they exchange time location claim and only when the witness is encountered, the data is encountered. Based on the storage of location claim it is divided as follows:

- Unary Time Location Storage and Exchange which stores only one location claim to detect replicas
- Multi Time Location Storage and Exchange which stores only multiple location claim to detect replicas

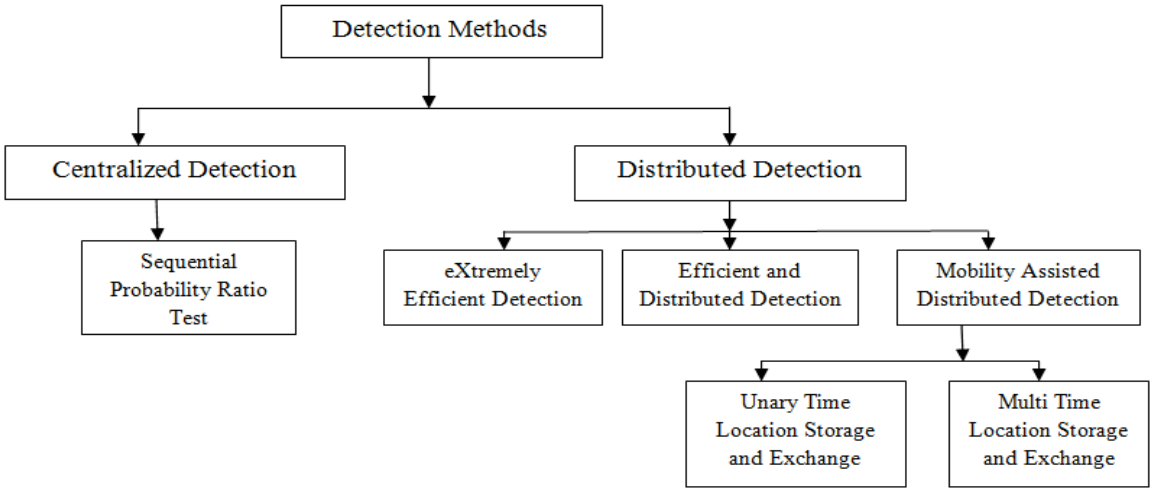

Fig 5: Clone Detection Methods in MSN

VII. CONCLUSION

In this survey, what is wireless sensor network, various characteristics of it and number of different various types of active attacks has been identified and addressed based on the threats and vulnerabilities of the active attacks in WSN. Also in this paper specifically attack is concentrated and various detection methods in mobile wireless sensor network environment are presented.

REFERENCES

[1] Chia-Mu Yu, Yao-Tung Tsou, Chun-Shien Lu, Sy-Yen Kuo, "Localized Algorithms for Detection of Node Replication Attacks in Mobile Sensor Networks", IEEE Transactions on Information Forensics and Security, 2013, pp 754-758.

[2] Mr. Madhav Bokare, and Mrs. Anagha Ralegaonkar, "Wireless Sensor Network," in International Journal of Computer Engineering Science (IJCES), Volume 2, Issue 3, March 2012.

[3] Dr. G. Padmavathi, Ms. L.S. Sindhuja, " Node Replication Attack in Mobile Wireless Sensor Networks: A survey," The International Journal of Computer Science & Applications (TIJCSA), Volume 2, No. 04, pp. – 2278-1080June 2013.

[4] Akhila Daniel and Preeja. V," A Survey on Detection of Clones in Wireless Sensor Networks," in International Journal of Computer Applications, Volume 91, No.7, April 2014.

[5] Dr. Shahriar Mohammadi1 and Hussein Jadidoleslamy," a comparison of physical attacks on Wireless sensor networks," International Journal of Peer to Peer Networks (IJP2P), Vol.2, No.2, April 2011

[6] Dr. G. Padmavathi and Mrs. D. Shanmugapriya," A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009