Clone Attacks in Wireless Sensor Networks: A Survey
Samridhi Madan1 Sandeep Kaushal2
1,2 Department of Electronics and Communication Engineering
1,2 Amritsar College of Engineering and Technology, Amritsar

Abstract—Sensor networks are highly distributed networks of small, lightweight wireless nodes, deployed in large numbers to monitor the environment or system by the measurement of physical parameters such as temperature, pressure, or relative humidity. Building sensors have been made possible by the recent advances in micro-electromechanical systems (MEMS) technology. The sensor nodes are similar to that of a computer with a processing unit, limited computational power, limited memory, sensors, a communication device and a power source in form of a battery. In a typical application, a WSN is scattered in a region where it is meant to collect data through its sensor nodes. The applications of sensor networks are endless, limited only by the human imagination.

Key words: Wireless sensor network, energy consumption, Clustering, cluster heads, Overheads

I. INTRODUCTION

Wireless sensor networks have become a growing area of research and development due to the tremendous number of applications that can greatly benefit from such systems and has led to the development of tiny, cheap, disposable and self-contained battery powered computers, known as sensor nodes or “motes”, which can accept input from an attached sensor, process this input data and transmit the results wirelessly to the transit network [1].

Wireless Sensor Networks (WSNs) can be defined as a self-configured and infrastructure-less wireless networks to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location or sink where the data can be observed and analysed. A sink or base station acts like an interface between users and the network. One can retrieve required information from the network by injecting queries and gathering results from the sink. Typically a wireless sensor network contains hundreds of thousands of sensor nodes. The sensor nodes can communicate among themselves using radio signals. A wireless sensor node is equipped with sensing and computing devices, radio transceivers and power components. The individual nodes in a wireless sensor network (WSN) are inherently resource constrained: they have limited processing speed, storage capacity, and communication bandwidth. After the sensor nodes are deployed, they are responsible for self-organizing an appropriate network infrastructure often with multi-hop communication with them. Then the on board sensors start collecting information of interest. Wireless sensor devices also respond to queries sent from a “control site” to perform specific instructions or provide sensing samples. The working mode of the sensor nodes may be either continuous or event driven. Global Positioning System (GPS) and local positioning algorithms can be used to obtain location and positioning information. Wireless sensor devices can be equipped with actuators to “act” upon certain conditions.

These networks are sometimes more specifically referred as Wireless Sensor and Actuator Networks [2].

Wireless networks are susceptible to security attacks due to the broadcast nature of the communication standard. Moreover, wireless sensor networks have an extra susceptibility because nodes are frequently placed in an aggressive or dangerous atmosphere where they are not actually safe.

Attacks on WSNs can be classified from two different levels of views [3]:
- Attack against security mechanisms.
- Attack against basic mechanisms (like routing mechanisms).

The attacks could be classified on the groundwork of the origin of the attacks i.e. Internal or External, and on the behavior of the attack i.e. Passive or Active attack. This classification is important because the attacker can exploit the network either as internal, external or/ as well as active or passive attack against the network.

A. Node Replication Attack (Clone Attack)

Conceptually, a node replication attack is relatively simple; an attacker pursues to complement a node to a prevailing sensor system by repetition the node ID of an existing node.

In this paper [4], a random key pre-distribution security schemes with little overhead are used and authors have presents hypothesis approach Bloom Filters to detect clone attacks in which a set of k symmetric keys are randomly selected from a pool of keys and then assigned to each node. Each node constructs a counting Bloom filter and sends its own filter to base station then BS take decision about the keys whose use exceeds the threshold value will be considered as a clone node. An algorithm is described in this paper can remove all cloned keys from the network when value of false positive rate is high.

II. RELATED WORKS

Several protocols have been proposed in the literature for clustering algorithms in WSN.

1) In this paper [4], a random key pre-distribution security schemes with little overhead are used and authors have presents hypothesis approach Bloom Filters to detect clone attacks in which a set of k symmetric keys are randomly selected from a pool of keys and then assigned to each node. Each node constructs a counting Bloom filter and sends its own filter to base station then BS take decision about the keys whose use exceeds the threshold value will be considered as a clone node. An algorithm is described in this paper can remove all cloned keys from the network when value of false positive rate is high.

2) In this paper [5], authors proposed a narrative scheme for detecting clone attacks in sensor networks, which works out for each sensor a collective fingerprint by extracting the region uniqueness, and verifies the authenticity of the initiator for each message by inspecting the
enclosed fingerprint. This verification is done both at the base station and sensor nodes then provides best and efficient way to find clone attack in sensor networks.

(3) In this paper [6], randomly directed exploration protocol is proposed to detect node replication in network in which every node has to keep its neighbour’s information and then collaborates to further claiming messages for finding out clone node. Practically, this protocol consumes low communication overhead and achieves high detection probability.

(4) In this paper [7], firstly, authors shows that in order to avoid the shortcomings of existing approaches, node-replica detection protocols must be non-deterministic and fully distributed (NDFD) and fulfil three security necessities on witness choice and they find that Randomized Multicast is the only protocol which is NDFD and fulfil the requirements but having high communication overhead. Then they proposed two new NDFD protocols, Random Walk (RAWL) and Table-assisted Random Walk (TRAWL) in this paper having moderate communication and memory overheads. Simulation results show that RAWL and TRAWL has lowest overheads in witness selection and also TRAWL is used to decrease the memory overhead of RAWL.

(5) In this paper [8], authors have proposed a lightweight method for clone detection in which clone nodes are notable by channel replies between nodes. The proposed system aims at attaining fast detection and minimizing the data transmission overhead by following the idea of spatial variability characteristic of wireless channels. Simulation results demonstrated that proposed method having low memory requirements and high detection probability.

(6) In this paper [9], authors describes that few distributed solutions were proposed for detection of clone attacks in network but these solutions are not satisfactory because of demanding more energy and memory. Authors also shows that these solutions do not completely meet network requirements then they propose a new self-healing, Randomized, Efficient and Distributed (RED) protocol. In this paper, authors analytically proved that RED produced less overhead than LSM and also maintain a balance between the nodes. RED is together ID-oblivious and area-oblivious so it is more flexible than LSM in detection capability.

(7) In this paper [10], authors have discussed various detection schemes for detection of replication attack and they suggested that distributed approach is more advantages than centralized approaches because there is a problem of single point failure in centralized schemes and many more. The approaches defined in this paper are dealt with only static networks, so for mobile WSN these approaches might be complex and cannot be suitable because of location changes time to time in mobile sensor networks.

(8) In this paper [12], a new method is proposed that is Area-Based Clustering Detection (ABCD) for detection of clone attacks. A comparison is done between this proposed method and distributed method namely Line-Selected Multicast (LSM) and it is found that proposed method provides high detection rate with less communication overheads than LSM. Simulation results shows that this proposed method ABCD is simple and efficient for detection of clone attack and can helps to decrease the number of stored messages when compared with centralized scheme with improving the network lifetime.

(9) In this paper [13], authors describes that wireless sensor networks are deployed in hostile environment so they are vulnerable to physical attack and one of the important and dreadful physical attacks is node clone attack in which an adversary attacks on a node, extracts secrets from it and make a copies of it in the entire network. Various node clone attack detection schemes are based on static sensor networks but in this paper a protocol is proposed namely Single Hop Detection (SHD) which is fully distributed and specially designed for mobile WSNs.

(10) In this paper [14], authors surveyed most existing clone detection schemes in WSNs in respect of device types, detection methodologies, deployment strategies and detection ranges and then their selection criteria based on static and dynamic wireless sensor networks. Simulation experiments carry out their comparison and they evaluated that grid deployment knowledge can save energy in static networks as compared to RM and LSM and on the other side there are high detection errors produced by many schemes in mobile WSNs.

(11) In this paper [15], authors present two distributed detection protocols: one is based on distributed hash table (DHT) that provides key-based routing and checking system to detect clone node in network with high security level and other is randomly directed exploration that presents superlative communication performance with minimal storage requirement.

III. ACKNOWLEDGMENTS

The paper has been written with the kind assistance, guidance and active support of my department who have helped me in this work. I would like to thank all the individuals whose encouragement and support has made the completion of this work possible.

REFERENCES


International Conference on Mechatronics and Automation, 372–376


