International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

A Review on Various Approaches for Routing & Attack Detection in WSN

Kulwinder Singh[1], Sheenam Malhotra[2]

[1]Department of Computer Science and Engineering, SGGSWU, Fathegarh Sahib

[2]Assistant Professor, Department of Computer Science and Engineering, SGGSWU, Fathegarh Sahib

Abstract: ***A wireless sensor network is a group of specialized transducers with a communications infrastructure for monitoring and recording conditions at diverse locations. The more modern networks are bi-directional also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance today such networks are used in many industrial and consumer applications, such as industrial process monitoring a control, machine health monitoring, and so on. The wireless sensor networks are made spatially distributed autonomous sensors to monitor physical or environmental conditions such as temperature, sound, pressure etc. and to cooperatively pass their data through the network to a main location.***

Keywords: wireless sensor network, cluster head, leaches protocol

1. Introduction

1.1 Wireless Sensor Network

A wireless sensor network is a group of specialized transducers with a communications infrastructure for monitoring and recording conditions at diverse locations. Commonly monitored parameters are temperature, humidity, pressure, wind direction and speed, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentrations, pollutant levels and vital body functions.

Figure 1.1: Wireless Sensor Networks

Wireless sensor network grows and rapidly improves, This enable the new communication service whenever we need to install a sensor network then it must fast, easy to install and maintain. Sensor network basically consist of large amount of sensor nodes that deployed to large physical area to monitor and detect the real time environmental activities [1].

The WSN is built of "nodes" from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "nodes" of genuine microscopic dimensions have yet to be created [3].A sensor network has limited computing and communication resources. To overcome this barrier, collaboration with surrounding nodes is required. In other words, information sharing between hierarchies is required rather than a hierarchicalapproach. A sensor network generally consists of a large number of sensor nodes for exact sensing and extendibility of sensing areas [5].It consists in replicating and deploying the captured sensors to launch a variety of malicious activities [4].This figure illustrates the wireless communication of WSN.

Wireless sensor network has resource constraints like limited battery supply (energy), low processing power, low storage, and low communication bandwidth. Applications of wireless sensor network include military surveillance, monitoring, health monitoring, structural monitoring etc. [2].

1.2WSNs can be divided in two classes:

1.2.1 Structured WSN

All or some of the sensor nodes are deployed in a pre-planned manner at fixed locations. The advantage of a structured WSN is that fewer devices can be deployed with lower network maintenance and management costs.

1.2.2 Unstructured WSN

Contains a dense collection of sensor nodes, which are randomly placed into the field .An ad-hoc deployment is preferred over a pre-planned deployment when the network is composed of hundreds to thousands of nodes in order to cover a larger area or when the environment is not directly accessible by humans attempting to construct WSN, e.g. Polar Regions, deep sea, or disaster areas such as a nuclear accident area or a war zone. WSNs have important applications such as remote environmental monitoring and target tracking. Now these days this has been enabled by the availability of sensors that are smaller, cheaper, and intelligent. These sensors are equipped with wireless interfaces with which they can communicate with one another to form a network.

1.3 Applications of Wireless Sensor Network

1.3.1 Process Management
The common application of WSN is area monitoring. In area monitoring, the WSN is deployed upon an area where some phenomenon is to be monitored. The use of sensors detects enemy intrusion is mil; a civilian example is the geo-fencing of gas or oil pipelines. Area monitoring is most important part.

1.3.2 Health care monitoring
The medical application of two types: wearable and implanted. First device are used on the body surface of a human and also just at close proximity of the user. The implantable medical devices are those which are inserted within the human body. There are also many other application like body position measurement and location of the person, overall monitoring of ill patients in hospitals and at homes. Body-area networks can collect information about an individual's health, fitness, and energy expenditure.

1.3.3 Environmental/Earth sensing
In monitoring environment there is so much application, examples of which are given below. They share the extra challenges of harsh environments and reduced power supply.

1.3.4 Air pollution monitoring
Wireless sensor networks have been deployed in several cities to monitor the concentration of dangerous gases for citizens. These can take advantage of the ad hoc wireless links rather than wired installations, which also make them more mobile for testing readings in different areas.

1.3.5 Forest fire detection
A network of Sensor Nodes can be installed in a forest to detect when a fire has started. The nodes can be equipped with sensors to measure temperature, humidity and gases which are produced by fire in the trees or vegetation. The early detection is crucial for a successful action of the firefighters; thanks to Wireless Sensor Networks, the fire brigade will be able to know when a fire is started and how it is spreading.

2. Review f Literature

Ruchi Mittal, M.P.S Bhatia [1] The Area of sensor network is very wide and used in various applications. There has been much work done in data mining sensor network, data stream etc. but very less work has been done at the combination of these areas. So introduce the combination of wireless sensor network and data mining to get some interesting and fresh results.

The beauty of sensor networking protocols is that they attracted a tremendous amount of research effort. For large sensor network the management of sensor database is itself a big task. Query processing techniques have been proposed for acquiring and managing sensor data. One major research goal of this problem in the database community is to efficiently detect outliers in are a large-scale database.

Yong-silk choi, et al [2]this paper suggests an inter-connective attestation protocol for sensor node suitable for wireless sensor network. This protocol is able to earlier detect a node that was damaged through neighbour node under a sensor network environment without a reliable sensor node. This protocol is for safe authentication for a sensor node. Existing research has focused on inter-connective authentication for sensor nodes and the BS instead of inter-connective authentication between sensor nodes. Therefore, when a sensor node is captured and viciously modified, the action consequently results in problems in the network environment. The existing attestation method uses a method that proves the code of sensor node through data collective characteristics for the sensor network.

VaibhavDeshpande,et al [3] Lifetime extension of wireless sensor network [1] uses two cluster heads and hierarchical routing. In this paper an algorithm with Two Cluster Head Energy efficient Wireless Sensor Network (TCHE-WSN) is proposed to improve the lifetime. The use of two cluster heads analogy reduces the overhead of single cluster head, avoids packet collision and improves reliable data transmission. In Energy Balanced Clustering in Wireless Sensor Network [2], algorithms for balanced cluster formation, cluster head selection, intra cluster and inter cluster communication are proposed to prolong lifetime of wireless sensor network. The performance of energy balanced clustering algorithm is compared with LEACH and EEMC protocol .In Energy Adaptive Cluster-Head Selection [3], optimization of LEACH's random cluster-head selection algorithm is proposed. It ensures that energy depletion over the whole network is balanced to prolong the network lifetime. Energy Consumption and lifetime analysis in clustered multi-hop wireless sensor networks [4] uses the probabilistic cluster-head selection mechanism. In this paper a novel energy model is proposed estimate the energy consumed in a multihop WSN.

M. Conti, et al [4]this paper focus on to several security attacks. In this work we focus on security of WSN .In particular, we cope with fundamental, specific, dreadful security attack mobile WSN are subject to, the so-called clone attack .It consists in replicating and deploying the captured sensors to launch variety of malicious activities.

Nikilmarriwala,et al [5]The LEACH routing protocol is developed by Dr. Wendi RabnirHeinzelmanin 2000[1], which uses the clustering and clustering task is rotated in the LEACHand cluster heads are selected randomly. LEACH is basedon aggregation technique that combines or aggregates theoriginal data into a smaller size of data that carry only meaningful information to all individual sensors. LEACH divides the wireless sensor network into several clusters.

Muhammad Arshad, et al [6] this paper explains a comprehensive comparison ofinter-cluster routing strategy, in terms of single and multi-hop communication for mobile WSN environmental applications. This guides throughput, network lifetime, packet loss ratio and end-to-end delay among the sensor nodes to base station. The basic parameters of networks are: Fixed base station which is far away from the sensors nodes, Homogenous and energy controlled sensor nodes and no high-energy nodes during the communication. Data fusion is best approach to avoid

information overload which is used in different hierarchical cluster based routing protocols.

3. Approaches Used

LEACH protocol: Low Energy Adaptive Clustering Hierarchy ("LEACH") is a TDMA-based MAC protocol which is integrated with clustering and a simple routing protocol in wireless sensor networks (WSNs). The goal of LEACH is to lower the energy consumption required to create and maintain clusters in order to improve the life time of a wireless sensor network. LEACH is based on aggregation technique that combines or aggregates the original data into a smaller size of data that carry only information to all individual sensors. LEACH divides the wireless sensor network into several clusters. Each cluster has a cluster head that aggregate the data from the cluster nodes and process the data and transmit it to the base station. LEACH uses a randomize rotation of high-energy CH position rather than selecting in fix manner [3].

Mobile-LEACH (M-LEACH): LEACH considers all nodes are homogeneous with respect to energy which is not realistic approach. In particular round uneven nodes are attached to multiple Cluster-head; in this case cluster-head with large number of member ode will drain its energy as compare to cluster-head with smaller number of associated member nodes. Furthermore mobility support is another issue with LEACH routing protocol. M-LEACH allows mobility of non-cluster-head nodes and cluster-head during the setup and steady state phase. MLEACH also considers remaining energy of the node in selection of cluster-head. Some assumptions are also assumed in M-LEACH like other clustering routing protocols. Initially all nodes are homogeneous in sense of antenna gain, all nodes have their location information through GPS and Base station is considered fixed in M-LEACH.

TL-LEACH: Two levels of the hierarchy LEACH (or TL-LEACH) is a proposed extension of the algorithm of LEACH which support parent child combination and then transmits data to base station by single hop fashion. It uses two levels of cluster heads (primary and secondary), and other simple detection nodes. In this algorithm, the primary cluster head in each group communicates with the secondaryand the contact with corresponding nodes in their sub cluster [6].

C-Leach: The disadvantage to LEACH is that the number of cluster head nodes is little ambiguous to count. LEACH-C has been proposed to clarify this problem. LEACH-C provides an efficient clustering configuration algorithm, in which an optimum cluster head is selected with minimization of data transmission energy between a cluster head and other nodes in a cluster. In LEACH-C, the base station receives information about residual node energy and node positions at the set up phase of each round. The received data can compute an average residual energy for all nodes. The nodes with less than average energy are excluded in selection of cluster heads. Among the nodes that have more than average energy, cluster heads are selected with use of the simulated annealing algorithm. The base station sends all nodes a message of the optimum cluster head IDs (Identifiers). The node, the ID of which is the same as the optimum cluster head ID, is nominated as a cluster head and prepares a TDMA schedule for data transfer. Other nodes wait for the TDMA schedule from their cluster heads

PEGASIS: PEGASIS is a routing protocol in which a chain based approach is followed. This protocol follows a greedy algorithm starting from the farthest node and all the sensor nodes form a chain like structure. It works on the principle that each node will transmit to and receive from its close neighbors. There is a leader in the chain which is responsible for transmission of the combined data to the sink node. Nodes take turns being the leader in the network which evenly distributes the energy load amongst the nodes. This even energy distribution and high energy efficiency leads to the extension of the network lifetime. It attempts to reduce the delay that the data acquires on the way to the base station.

4. Problem Formulation

In the wireless sensor networks the network nodes are used for the sensing the information from the various types of non-reachable areas. Wireless sensor nodes has been used for the sensing the information from harsh environment. In these nodes sensors of different types has been used for collecting information. Wireless sensor networks are of main two types, which are static wireless sensor nodes and mobility wireless sensor networks. In MWSNs the main threat in the network is security. Various types of attacks occurred in these networks. Attack occur in WSN is clone attack which is also known as replica attack. In this attack the node copy the id of the other node and show its predictions at different locations. A clone node can create a black hole or wormhole attack include adversary can use them in different ways. This attack can transmit false information to all legitimate nodes. The clone attack is very suitable for adversary. For this attack adversary has not to be compromise for number of nodes. The adversary can do cloning of one node and can predict other nodes through this node. It falsifies its positions at different times at different locations. Main problem in this is to detect the node having clone attack, because each and every node has same id and locations at different position on same interval of time. This problem has also been arising in clusters in which clusters replicate and the main problem arises when cluster head replicate. This figure illustrates the detection of clone node.

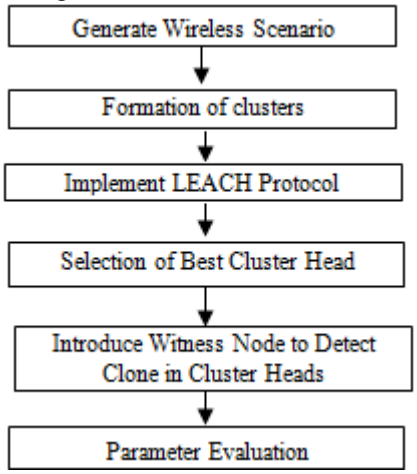

Figure 1.2: Detection of clone node

5. Conclusion

In the wireless sensor networks the network nodes are used for the sensing the information from the various types of non-reachable areas. In MWSNs the main threat in the network is security. Various types of attacks occurred in these networks. Attack occur in WSN is clone attack which is also known as replica attack. In this attack the node copy the id of the other node and show its predictions at different locations. A clone node can create a black hole or wormhole attack include adversary can use them in different ways. This attack can transmit false information to all legitimate nodes. The clone attack is very suitable for adversary. For this attack adversary has not to be compromise for number of nodes. The adversary can do cloning of one node and can predict other nodes through this node. It falsifies its positions at different times at different locations. Main problem in this is to detect the node having clone attack, because each and every node has same id and locations at different position on same interval of time. This problem has also been arising in clusters in which clusters replicate and the main problem arises when cluster head replicate.

References

[1] Ruchimittal M.P.S Bhatia,"Wireless sensor networks for monitoring the environmental activities, International conference on distributed computing and network(ICDCN),Vol.38, PP.:393-422,india,2010.
[2] Deshpande, V.V Garg,"Energy efficient clustering in wireless sensor network using cluster of cluster heads, IEEE Conference on Wireless and Optical Communications Networks (WOCN), Vol.1 , no.13, PP.: 5999-3,India,2013.
[3] Nikhil Marriwala, "An approach to increase the wireless sensor network lifetime, IEEE, Vol. 3, India, 2012.
[4]]M. Conti R.DiPietro,A.Spognardi, "Wireless sensor replica detection in mobile network",Thirteen international conference on distributed computing and networking, International conference on distributed computing and network(ICDCN),PP.:249-264,Rome,Italy,2012.
[5] Yong-Silk Choi Young –Jun jeon, Sng-Hyun park "A study on sensor nodes attestation protocol in a wireless sensor network, ICACT, PP.:7-10, SouthKorea, 2010.
[6] MuhammadArshad, Naufal M. Saad, "Routing strategies in hierarchical cluster based mobile wireless sensor networks, IEEE, PP.:230-, Pahang, Malaysia, June 21-22, 2011.