International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Reduction of Energy Consumption and Attack Prevention in Mobile Wireless Sensor Network: A Review

Ashe Kiran[1], Deepinder Dhaliwal[2]

Research Scholar at DBU, Mandi Gobindgarh, Punjab, India

Assistant Professor, DBU, MandiGobindgarh, Pb., India

Abstract: ***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.***

Keywords: WSN, Clone attack, Security, Clustering.

1. Introduction

1.1 Wireless Sensor Network

Sensor networks are connected with these that are used to sense the information from the location where network is deployed each node contain multiple parts a radio trans-receiver with an internal antenna or connection to an external antenna. A microcontroller, an electric circuit to interface with the sensors has been used for sensing and an energy source is used. When we provide energy to WSN nodes maximum a battery of cells is used. According to situation the size of the sensor node is calculated and location it can be of grain dust size to the size of shoe box. The cost of sensor nodes varies according to the characteristics, energy, communication range and bandwidth used for communication. The technology which used WSN transfer from star topology to multi hop wireless mesh topology. Mobile WSN is a type of network in which the sensor nodes which are used for sensing are mobile. The mobile means that the nodes can move throughout the network.

1.2 MWSN

Mobile wireless sensor network (MWSNs) can basically be characterized as a wireless sensor network (WSN) in which the sensor hubs are portable. MWSNs are a littler, developing field of exploration as opposed to their entrenched ancestor. MWSNs are significantly more adaptable than static sensor systems as they can be sent in any situation and adapt to fast topology changes. On the other hand, a significant number of their applications are comparative, for example, environment checking or reconnaissance usually the hubs comprise of a radio handset and a microcontroller controlled by a battery. And additionally some sort of sensor for distinguishing light, warm, stickiness, temperature, and so forth.

1.3Clustering

Clustering is the task of grouping a set of objects in such a way that objects in the same group (called a cluster) are more similar (in some sense or another) to each other than to those in other groups (clusters). It is a main task of exploratory data mining, and a common technique for statisticaldata analysis, used in many fields, including machine learning, pattern recognition, image analysis, information retrieval, and bioinformatics.

Cluster analysis itself is not one specific algorithm, but the general task to be solved. It can be achieved by various algorithms that differ significantly in their notion of what constitutes a cluster and how to efficiently find them. Popular notions of clusters include groups with small distances among the cluster members, dense areas of the data space, intervals or particular statistical distributions. Clustering can therefore be formulated as a multi-objective optimization problem

1.4Energy Dissipation Model in WSN

1) Data Acquisition and No Processing (DANP) approach
2) Data Acquisition and Transform Coding (DATC) approach
3) Data Acquisition and Compressive Sensing (DACS) approach

1.4.1 Compressive Sensing

Wireless Sensor Networks (WSNs) are comprised of spatially distributed sensor nodes, where each node contains units for sensing, processing, and communicating data. In general, sensor nodes are assumed to have limited processing power and highly constrained energy resources. A typical WSN topology includes a base station - a powerful entity more capable than the ordinary sensor nodes with a significantly higher energy budget. Ordinary sensor nodes

transfer processed or raw sensed data to the base station, which performs the final information aggregation and extraction tasks.

1.4.2 Mixed Integrated Programming

Mixed Integer Programming (MIP) based analysis of communication networks is extremely useful for uncovering the fundamental performance limits. Choosing an MIP based analysis method has a number of advantages. One of them is the abstraction from a specific protocol which enables us to investigate energy cost in ideal conditions with optimal routing decisions. Secondly, due to global knowledge in the optimization problem solver, the results can be obtained in an efficient and consistent manner.

1.5 Routing Protocols

Reactive Protocol: Reactive protocol searches for the route in an on-demand manner and set the link in order to send out and accept the packet from a source node to destination node. Route discovery process is used in on demand routing by flooding the route request (RREQ) packets throughout the network. Examples of reactive routing protocols are the dynamic source Routing (DSR), ad hoc on-demand distance vector routing (AODV).

Proactive Protocol: Each node in the network has routing table for the broadcast of the data packets and want to establish connection to other nodes in the network. These nodes record for all the presented destinations, number of hops required to arrive at each destination in the routing table. The routing entry is tagged with a sequence number which is created by the destination node. To retain the stability, each station broadcasts and modifies its routing table from time to time. How many hops are required to arrive that particular node and which stations are accessible is result of broadcasting of packets between nodes.

2. Review of Literature

WassimZnaidi et al [1] "Hierarchical Node Replication Attacks Detection in Wireless Sensor Networks",Wireless sensor networks (WSNs) are composed of numerous low-cost, low-power sensor nodes communicating at short distance through wireless links. Sensors are densely deployed to collect and transmit data of the physical world to one or few destinations called the sinks. Because of open deployment in hostile environment and the use of low-cost materials, powerful adversaries could capture them to extract sensitive information (encryption keys, identities, addresses, etc.). When nodes may be compromised, "beyond cryptography" algorithmic solutions must be envisaged to complement the cryptographic solutions. This paper addresses the problem of nodes replication; that is, an adversary captures one or several nodes and inserts duplicated nodes at any location in the network. If no specific detection mechanisms are established, the attacker could lead many insidious attacks

JaydeepBarad et al [2] "improvement of deterministic key management scheme for securing cluster-based sensor networks" As sensor nodes are deployed in hostile or remote environment and unattended by human, they are prone to different kind of attacks. So adaptation of dynamic key is very important for secure key management, for encrypting messages for communication. Because of the limitations of WSN like limited memory, battery life and processing power, use of cluster-based wireless sensor network reduces system delay and energy consumption. For the same, LEACH, cluster based protocol for sensor networks, achieves energy efficient and scalable routing. Whereas storage issue in sensor network, can be reduced by using deterministic key management scheme. In this context, from all the different key management schemes in WSNs, deterministic key management scheme with LEACH, called DKS-LEACH is the scheme which is used to secure wireless sensor network in efficient manner and provides authentication, confidentiality and integrity of sensed data. Still energy consumption and resilience against node capture is an issue with DKS-LEACH. So we proposed the scheme RINGLEACH to improve the existing scheme to make it more resilient using distance based key management scheme.

NayyerPanahi et al [3] "Adaptation of LEACH Routing Protocol to Cognitive Radio Sensor Networks" One of the drawbacks of LEACH protocol is the uncontrolled selection of cluster heads which, in some rounds, leads to the concentration of them in a limited area due to the randomness of the selection procedure. LEACH-C is a variant of LEACH that uses a centralized clustering algorithm and forms good clusters through sink control. According to experimental results, the IEEE 802.15.4 packets are damaged by WLAN interferences in ISM band. It seems that, sensor nodes equipped with cognitive radio capabilities can overcome this problem. In cognitive radio sensor networks (CRSN), routing must be accompanied by channel allocation. This requires spectrum management which can be devolved to cluster heads. For this networks, new duty cycle mechanisms must be designed that jointly consider neighbor discovery, and spectrum sensing/allocation. Cluster-based network architecture is a good choice for effective dynamic spectrum management. In such architecture, cluster heads have a proper spatial distribution and are optimally located all over the network

mr.suyogpawar et al [4] "design and evaluation of en-leach routing protocol for wireless sensor network" A wireless network consisting of a large number of small sensors with low-power transceivers can be an effective tool for gathering data in a variety of environments like civil and military applications. The data collected by each sensor is communicated through the network to a single processing centre called base station that uses all reported data to determine characteristics of the environment or detect an event. Clustering sensors into groups, so that sensors communicate information only to local cluster-heads and then the cluster heads communicate the aggregated information to the processing center, may save a lot of energy. LEACH is clustering based protocol that utilizes randomized rotation of local cluster-heads to evenly distribute the energy load among the sensors in the network.

Shin-nosuke Toyoda et al [5] "Dynamic Change Method of Cluster Size in WSN" One of the major issues in wireless sensor network isdeveloping an energy-efficient routing

protocol. LEACH isvery energy-efficient routing protocol based on the clustering of the sensor nodes. However, energy consumption of nodes tends to become uneven in LEACH. HEED improves the LEACH clustering algorithm by using information of residual electric power of nodes. Although HEED provides better performance than LEACH, it does not consider the number of adjacent nodes. Therefore, the cluster head does not efficiently cover the nodes in HEED.HIT is based on the small transmission range and multi- hop communication. Though HIT has improved the performance dramatically, unbalance of the electric power consumption is remained. In this paper, we propose energy- efficient clustering algorithm considering adjacentnodes and residual electric power.

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 a hierarchical protocol in which most nodes transmit to cluster heads, and the cluster heads aggregate and compress the data and forward it to the base station. Each node uses a stochastic algorithm at each round to determine whether it will become a cluster head in this round. LEACH assumes that each node has a radio powerful enough to directly reach the base station or the nearest cluster head, but that using this radio at full power all the time would waste energy.

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.

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. Conclusion

In the wireless sensor networks the network nodes are used for the sensing the information from the various types of non-reachable areas. 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. In this we used Leach Protocol. LEACH is a hierarchical protocol in which most nodes transmit to cluster heads, and the cluster heads aggregate and compress the data and forward it to the base station (sink). Each node uses a stochastic algorithm at each round to determine whether it will become a cluster head in this round.

References

[1] WassimZnaidi “Hierarchical Node Replication Attacks Detection in Wireless Sensor Networks”, *IEEE Conf. on Personal, Indoor and Mobile Radio Communications*, 2009, pp 82 – 86.
[2] JaydeepBarad“improvement of deterministic key management scheme for securing cluster-based sensor networks” *IEEE Conf. on Networks & Soft Computing (ICNSC)*, 2014, pp 55 – 59.
[3] NayyerPanahi “Adaptation of LEACH Routing Protocol to Cognitive Radio Sensor Networks*” IEEE Conf. on Telecommunications (IST)*, 2012, pp 541 – 547.
[4] *MR.SUYOG PAWAR* “design and evaluation of en-leach routing protocol for wireless sensor network*”*

IEEE Conf. on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2012,pp 489 – 492.

[5] Shin-nosuke Toyoda "Dynamic Change Method of Cluster Size in WSN" *IEEE Conf. on Broadband, Wireless Computing*, 2012, pp 20 – 27.

[6] muhammadhaneef "comparative analysis of classical routing protocol leach and its updated variants that improved network life time by addressing shortcomings in wireless sensor network", *IEEE conf. On Mobile Ad-hoc and Sensor Networks (MSN)*, 2011, pp 361 – 363.

[7] YingpeiZeng ; State Key Lab. for Novel Software Technol., Nanjing Univ., Nanjing, China ; Jiannong Cao ; Shigeng Zhang ; ShanqingGuo "Random-walk based approach to detect clone attacks in wireless sensor networks ", 0733-8716, 677 – 691, IEEE, 2013.

[8] Sivasankar, P.T.; Ramakrishnan, M. "Active key management scheme to avoid clone attack in wireless sensor network"

[9] U. Ahmed and F.B. Hussain, "Energy efficient routing protocol for zone based mobile sensor networks", in proceedings of the 7th international Wireless Communications and Mobile Computing conference (IWCMC), pp. 1081-1086.

[10] Y. Han and Z. Lin. "A geographically opportunistic routing protocol used in mobile wireless sensor networks", in proceedings of the 9th IEEE international conference on Networking, Sensing and Control (ICNSC), pp. 216-221.