Volume 5, Issue 5, May 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Enhancing LEACH Protocol for Detection of Clone Attacks in Wireless Sensor Networks

Ramneet Singh, Lal Chand
Department of Computer Engineering
Punjabi University, Punjab, India

***Abstract** - Wireless Sensor Networks are self-configured networks consisting of number of tiny low-cost sensor nodes. These nodes are used to monitor various changes occurring in a particular environment. Since these networks are deployed in vigorous physical conditions, the sensor nodes are prone to various types of attacks and clone attack is one of them. Various clone detection techniques have been proposed so as to maintain the efficiency of wireless sensor networks. LEACH (Low Energy Adaptive Clustering Hierarchy) protocol is an integration of clustering and simple routing which aims to lower the energy consumption and provides maintenance of clusters in wireless sensor networks. In this paper, we will propose a new method that is enhanced LEACH protocol by increasing its energy efficiency and also making it more secure using CA (Certification Authority) technique for selecting cluster heads and authenticating each and every node in the network. Then we will try to detect clone attacks in the network and provide simulation results based on different parameters.*

***Keywords** - Wireless sensor networks, security, certification authority, enhanced LEACH, clone detection.*

I. INTRODUCTION

Wireless sensor networks are implemented for monitoring physical and environmental conditions such as temperature, sound, motion, pressure etc. and then collectively passing the data to a base station where the data can be analysed. The base station acts like an interface between the user and the network. A wireless sensor network consists of several number of tiny, low cost sensor nodes which are deployed in very competitive environment for performing monitoring related tasks. Wireless sensor nodes use radio signals for communicating with each other. The main components of a wireless sensor node are: a microcontroller which performs tasks, processes the data and also controls the functionality of other components in the network; a transceiver which provides radio frequency based communication in the wireless sensor network; external memory for storing application or programming data as well information related to the identification of the node; a power source to provide adequate energy for communication process; sensors for measuring the physical data to be monitored. The components of a sensor node are shown in the given figure. Due to the low cost of the wireless sensor node, it is possible to deploy thousands of sensor nodes in a particular area.

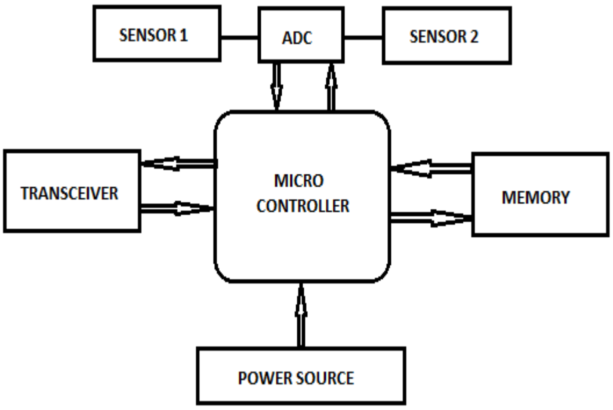

Fig.1 Components of a wireless sensor node.

These nodes require minimal amount of supervision and it is very challenging to provide efficient security functions and mechanisms for WSNs.

These sensor nodes are deployed in very aggressive environments and can be captured and compromised very easily. From a compromised node, all of its secret credentials are extracted by an adversary such as node id, nodes location, keys etc. This process is done create a replicated node against that captured node and after that large number of replicated nodes are introduced into that deployment area. Usually this is done so that an attacker can expand the compromised area and employing clones to perform attack on the network. This phenomenon of capturing a node and extracting its information to build a replica node is known as a clone attack. The replica nodes could be authenticated as legitimate node and to launch various types of attacks like injecting false data, corrupting data aggregation, dropping data packets selectively. Thus, it is essential to detect clone nodes promptly for minimizing their damages to WSNs. Therefore, clone attackers are severely harsh and efficient and effective solutions for clone attack detection are needed to limit their harms.

Various techniques have been proposed for detection of clone attacks in wireless sensor networks. Certainly these techniques provide an efficient mechanism for clone detection but still there is always scope for advancement. LEACH (Low Energy Adaptive Clustering Hierarchy) protocol is an integration of clustering and simple routing which aims to lower the energy consumption and provides maintenance of clusters in wireless sensor networks. All nodes that are not cluster heads only communicate with the cluster head according to the schedule created by the cluster head. Cluster head is selected randomly in every rotation based on sensor node having highest energy. The cluster head communicates directly with sink or user. However, it does not determine that whether the node selected as cluster head [15] is trustworthy or not. The cluster head randomly selected could be prone to clone attack. Therefore, in this paper, we propose a new technique that enhances the working of LEACH protocol by employing a CA (Certification Authority) that provides digital certificate to each and every node in the network. When each and every node is authenticated using digital signature from certification authority, any clone node available in the network would not be selected as the cluster head and also the clone node would be discarded from being communicated with other nodes. So, we propose a technique that will enhance the security as well as improves the energy efficiency of the network. We will also provide simulation results at the end based on comparison between different parameters.

II. RELATED WORK

Clone detection techniques are classified as centralized and distributed techniques. In a centralized detection approach [3], the sensor nodes available in a wireless sensor network will send the locations and IDs of all their neighbors to a base station. The base station then verifies that each and every node should be at a distinct location. If a node with same id is detected at two different locations then there is a probability of replicated node in the network. On the other hand, in the distributed approach of clone detection, every node collects all of its neighbor's identities along with their locations and broadcasts to the network. Both categories have their own pros and cons.

In straightforward detection scheme given in [5], Parno et al. (2005) proposed that each node is required to send a list of its neighbors (along with their ids) and the positions claimed by these neighbors to the base station, which then examines every neighbor list to look for replicated sensor nodes. In a stationary WSN, conflicting position claims for one node id indicates a replication. Once the base station spots one or more replicas, it can revoke the replicated nodes by flooding the network with an authenticated revocation message. Cloned key detection [1] was proposed by Brooks et al. (2007). A clone detection protocol based on random pairwise key pre-distribution schemes was proposed. This method is used for detection of cloned keys rather than the replicated sensor nodes. A very efficient centralized technique known as the ABCD method [9] was proposed in which an area is divided into different sub-areas and for each area a witness node is allocated. All the nodes in a particular sub-area communicate through that witness node. The witness nodes then help in detecting and revoking the clone nodes in the network.

There are also several distributed clone detection techniques available. N2NB (Node-to-Network Broadcasting) is a very simple and efficient approach for clone detection in wireless sensor networks. In this method [7], every node gathers all its neighbors' ids and their positions, and broadcasts it to the entire network. When a broadcast message is received by the node, it compares those nodes listed in the message with its own neighbors. Once nodes that have conflicting positions are spotted, they can be revoked also with authenticated broadcasts. In Randomized Multicast (RM) [7] scheme each sensor announces its locations and each of its neighbors can send a copy of that claim to randomly selected nodes (i.e. witness node) and exploiting the birthday paradox effect to detect the clone nodes. (RAWL) was proposed in [8] in which each node broadcasts a signed location claim. The probability is that the neighbors of each node will forward its location claim to some randomly selected nodes. Each randomly selected node sends a message containing the claim to start a random walk in the network, and the passed nodes are selected as witness nodes and will store the claim. If any witness receives different location claims for a same node ID, it can use these claims to revoke the replicated node. LCA approach using deployment time interval is also a very efficient clone detection technique proposed in [6]. This approach is based on the grid deployment knowledge to detect the clone nodes by considering nodes location and ID. As far as enhancement of LEACH protocol is concerned, various techniques have been proposed for its improvement. N-LEACH is proposed in [13]. Trust based cluster head selection algorithm is proposed in [15]. Thus these are some of the related clone detection techniques. Now we will discuss about the proposed work in the next section.

III. PROPOSED WORK

LEACH (Low Energy Adaptive Clustering Hierarchy) is a protocol that provides simple routing and clustering in wireless sensor networks. Its main objective is to lower the energy consumption and maintain clusters in order to improve the lifetime of wireless sensor network. It is a hierarchical protocol in which most nodes transmit to cluster heads, and then the cluster heads forward it to the base station. The algorithm of LEACH protocol consists of:

- Cluster based
- Data aggregation at cluster head
- Random cluster head selection
- Cluster heads communicate directly with base station.

As we know, according to the simple LEACH protocol, the clusters heads are randomly elected in every rotation based on sensor node having highest energy. Various new methods have been proposed for improvement in LEACH protocol as in [12] [13]. However, it is not known that whether the node elected as cluster head is trustworthy or not. The node selected as cluster head may be prone to clone attack. So therefore, a certification authority [14] is allocated that will provide digital certificate to each and every node available in the wireless sensor network. The certification authority will authenticate every node so that any sensor node selected as cluster head is trustworthy. This will not only enhance the security of the wireless sensor network but will also improve its performance. The proposed work flow is given as:

- Cluster head selection using CA authority.
- Assignment of unique encrypted signature using digital certificate.
- Signature, ID & Location based Clone Detection
- Result Analysis

IV. SIMULATION SETUP

The proposed work have been evaluated for performance using Network Simulator (NS 2.35) which is a discrete event network simulator based on C++ and OTcl script. The plots are the result of simulation of wireless sensor network consisting number of nodes. Table I summarizes the parameters used by the simulator to create the WSN simulation environment.

Table 1: Simulation Parameters

Parameters	Values
Channel	Wireless
Propagation Model	Two Ray Ground
MAC	IEEE 802.11
Area	1800*1400
No. of Nodes	50
Simulation time	30 seconds

V. RESULTS AND DISCUSSIONS

The proposed work is simulated and tested for 50 nodes to evaluate the performance parameters. The nodes are spread in an 1800 m by 1400 m area. Simulations are run for 30 sec. The proposed work will be evaluated for the following metrics:-

- **Average end-to-end delay**: - The average end-to end delay is the average time taken between the generation of a packet by the source node and the time when this packet is received at the destination which includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation.

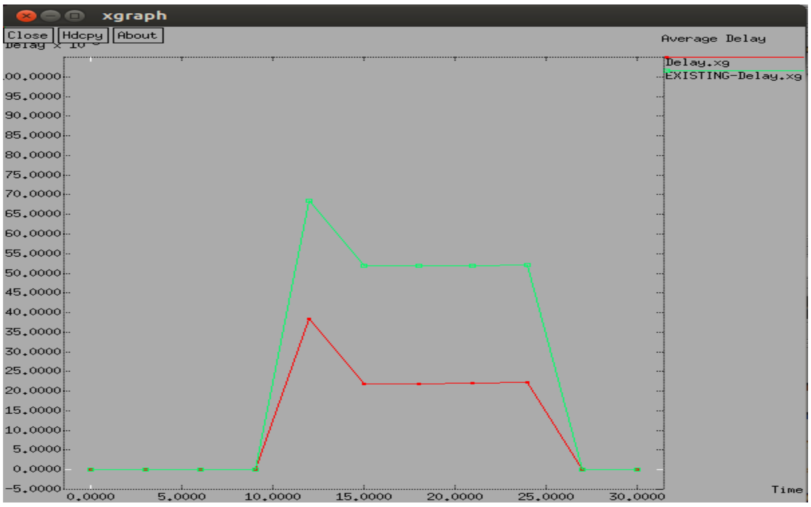

Figure 2: Average Delay

Figure 2 shows the delay output graphs simulated for an existing clone detection technique along with enhanced technique using certification authority but without clustering. Here we can see that when we allocated a certification authority, the average delay decreases as compared to the existing technique. Now we will compare the average delay with the enhanced LEACH technique in next figure. Figure 3 shows the comparison with the enhanced LEACH technique. In these figures, we can see that with the use of certification authority the average delay between the nodes keeps on decreasing which improves the efficiency of the network.

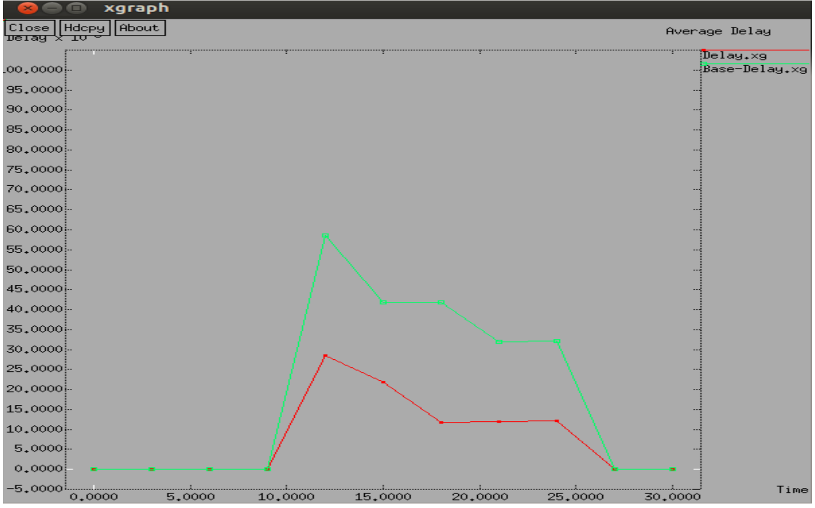

Figure 3: Average Delay for Enhanced LEACH

- **Packet delivery ratio**: - The Packet Delivery Ratio (PDR) metric is the number of packets successfully received by the destination node to the number of packets that was transmitted by the source nodes.

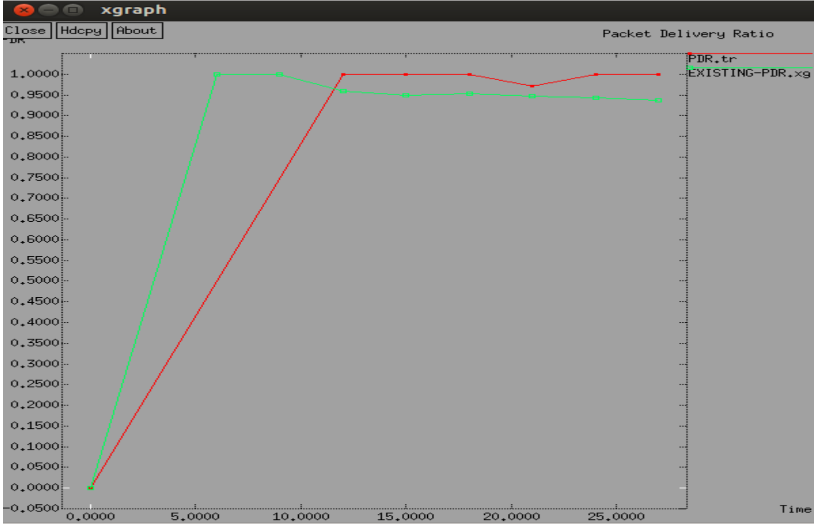

Figure 4: Packet Delivery Ratio

Figure 4 shows the packet delivery ratio output graphs simulated for an existing clone detection technique along with enhanced technique using certification authority but without clustering. Figure 5 shows the comparison with the enhanced LEACH technique. In these figures, we can see that with the use of certification authority the packet delivery ratio between the nodes keeps on increasing.

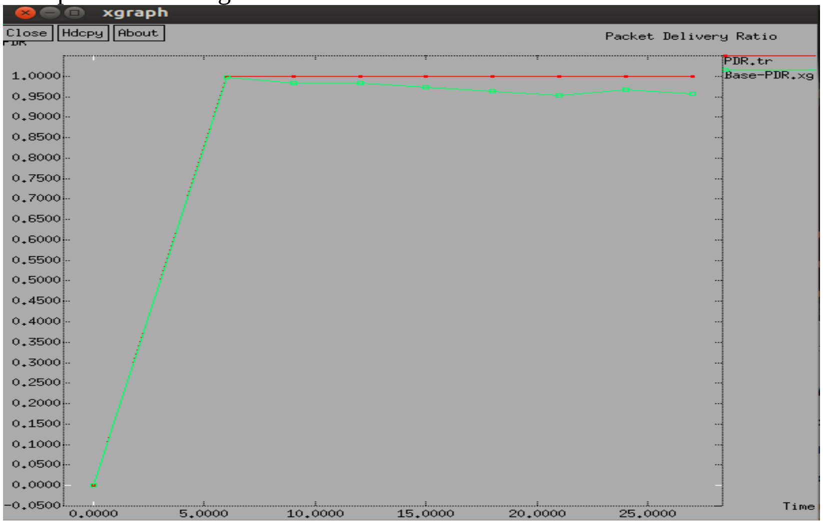

Figure 5: Packet Delivery Ratio for enhanced LEACH

- **Throughput**: - Throughput is the rate of successful message delivery over a communication channel or we can say number of data packets sent per second.

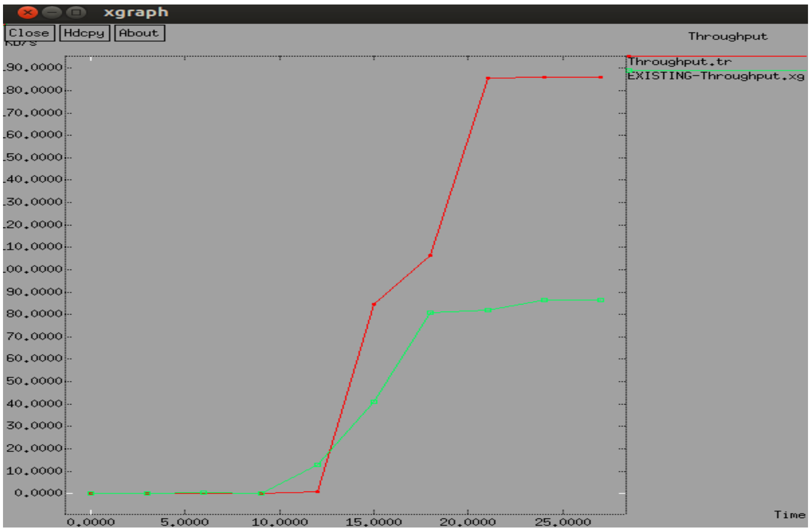

Figure 6: Throughput

Figure 6 shows throughput output graphs simulated for an existing clone detection technique along with enhanced technique using certification authority but without clustering and figure 7 shows the comparison of throughput with the enhanced LEACH technique. In these figures, we can see that with the use of certification authority the throughput between the nodes is increased.

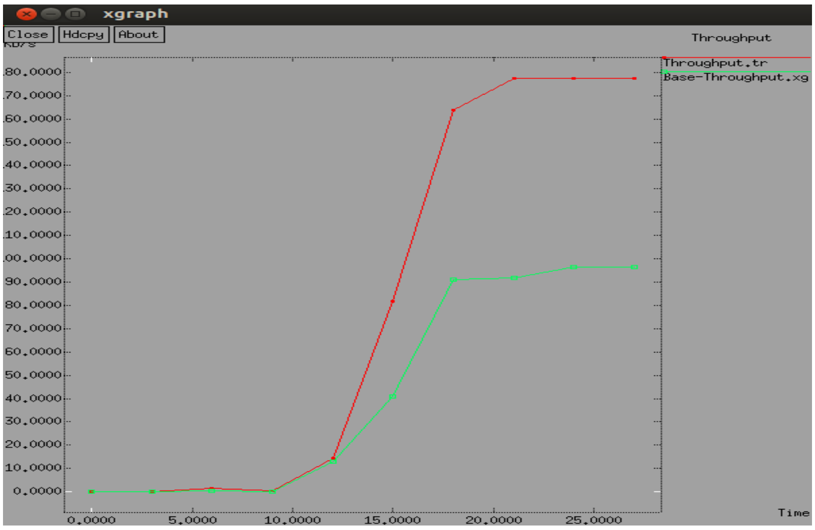

Figure 7: Throughput for enhanced LEACH

VI. CONCLUSIONS AND FUTURE SCOPE

In this paper, we discussed a major security issue of wireless sensor networks known as clone attacks and its detection. We classified some traditional and recently advanced detection protocols as centralized and distributed and reviewed the literature. LEACH is a very energy efficient protocol used in wireless sensor networks. So we tried to enhance its efficiency by employing a certification authority that provides digital certificate to each and every node in the network. This provides security to the network as for every round a trusty cluster head will be selected. We have also provided graphical results of various metrics compared. The average delay using this method is decreased whereas the packet delivery ratio and throughput is increased which results in improving the efficiency of the network. The main motive of recent research in this area is to find an optimal detection technique which helps in increasing the performance of network by reducing the costs and communication overheads. So, we hope that these techniques will provide complimentary mechanisms against clone attacks and help in enhancing the security aspect of wireless sensor networks.

REFERENCES

[1] Brooks R, Govindaraju PY, Piretti M, Vijaykrishnan N, Kandemir MT, “On the detection of clones in sensor networks using random key predistribution” IEEE 2007; 37(November): 1246-58.

[2] Choi H, Zhu S, La Porta TF, SET: Detecting node clones in sensor networks, In proceedings of the third international conferece on security and privacy in communications and networks and the workshops (Securecomm’07); 2007. P 341-50, December.

[3] D Sheela, Priyadarshini, Dr. G. Mahadevan, “Efficient approach to detect clone attacks in wireless sensor networks”, IEEE, 2011.

[4] Kwantae Cho, Minho Jo, Taekyoung Kwon, Hisao-Hwa Chen, Dong Hoon Lee, “Classification and experimental analysis for clone detection approaches in wireless sensor networks”, IEEE, Vol. 7, No. 1, March 2013.

[5] Parno B, Perrig A, Gligor V, “Dsitributed detection of node replication attacks in sensor networks.”, IEEE, p. 49-63, May 2005.

[6] R. Sivaraj, R. Thangarajan, “Location and Time based clone detection in wireless sensor networks”, IEEE, 2014.

[7] Wen Tao Zhu, Jianying Zhou, Robert H. Deng, Feng Bao, “Detecting node replication attacks in wireless sensor networks” *Elsevier*, 1022-1034, 2012.

[8] Yingpei Zeng, Jiannong Cao, “Random walk based approach to detect clone attacks in wireless sensor networks”, IEEE, Vol. 28, No. 5, June 2010.

[9] Wibhada Naruephipat, “An area-based approach for node replica detection in wireless sensor networks”, IEEE, 2012.

[10] Zhang M, Khanapure V, Chen S, Xiao X, Memory efficient protocols for detecting node replication attacks in wireless sensor networks, IEEE (ICNP’09); 2009. P. 284-93, October.

[11] Jennifer Yick, Biswanath Mukherjee, Deepak Ghosal, “Wireless Sensor Network Survey”, Elsevier, 2292-2330, 2008.

[12] Lalita Yadav, Ch. Sunitha, “Low Energy Adaptive Clustering Hierarchy in Wireless sensor networks” IJCSIT, 2014.

[13] Yuling Li, Luwei Ding, “The improvement of LEACH protocol in Wireless sensor network” IEEE 2011.

[14] An advanced security scheme based on clustering and key distribution in vehicular ad-hoc networks, Elsevier 2014.

[15] L. Ramalingam S. Audithan “Trust based cluster head selection algorithm for wireless sensor network”, IEEE 2014.