Energy Efficient in Clone Detection and Eavesdropper Mitigation Mechanism in WSN

V.Sathya[1], J. Priyadharshini[2], B. Aarthi[3], R. Kalaiselvi[4]
[1]Assistant Professor, [2 3 4]Final CSE,
A.V.C College of Engineering, Mannampandal-609 305

Abstract- *In many sensor network applications, such as environment monitoring systems, sensor nodes need to collect data periodically and transmit them to the data sink through multi hops. Compressive Sensing (CS) can reduce the number of data transmissions and balance the traffic load throughout networks. However, the total number of transmissions for data collection by using pure CS is still large. The hybrid method of using CS was proposed to reduce the number of transmissions in sensor networks. In this paper, we propose a clustering method that exploits better data aggregation techniques for large network but it leads to compromising attacks or clone attacks. The private information of the source node, i.e. identity and the location information are shared with witnesses at the stage of witness selection. Trust and Reputation systems are used to find the trust worthiness of the data aggregation from the cluster head and the cluster nodes. Further the energy efficiency is a challenge task for the sensor nodes here the mechanism may derive to perform sleep and wait methodology to improve the life time of the sensor nodes. The sniffers may implemented to monitor the energy of the sensor nodes periodically in the sink.*

Keyterms *—Wireless Sensor Networks, Clone duplicate verification messages. To make sure that Detection, Energy Efficiency, Compressive Sensing,Network Lifetime, Sniffers Management.*

I. INTRODUCTION

Wireless sensors have been widely deployed for a variety of applications, ranging from environment monitoring. For cost-effective sensor placement, sensors are usually not tamper-proof devices and are deployed in places without monitoring and protection, which makes them prone to different attacks. For example, a malicious user may compromise some sensors and acquire their private information. Then, it can duplicate the sensors and deploy clones in a wireless sensor network (WSN) to launch a variety of attacks which is referred to as the clone attack. As the duplicated sensors have the same information, e.g., code and cryptographic information, captured from legitimate sensors, they can easily participate in network operations and launch attacks. Due to the low cost for sensor duplication and deployment, clone attacks have become one of the most critical security issues in WSNs. Thus, it is essential to effectively detect clone attacks in order to ensure healthy operation of WSNs. Energy Efficient Ring Based Clone Detection (ERCD) protocol can balance the energy consumption of sensors at different locations. ERCD consists of two stages. They are: Witness should be randomly selected and At least one of the witnesses can successfully receive all the verification message(s) for clone detection.

The network region is separated into adjacent rings. ERCD protocol can achieve superior performance in terms of the clone detection probability and network lifetime. The main drawback of this is lack of concentration in sensor node clustering and the compromising attacks. The lifetime of the sensor is failed to improve and it does not balance the traffic node and also energy efficient is less.

To make it difficult for the eavesdropper the communication between the current source node and its witnesses, the CS technique is used. By using this technique the malicious users can not generate atleast one of the witness can check the identity of the sensor node and to determine whether there is a clone attack or not in this network, the clustered environment for data aggregation in wireless sensor network is provided along with that the energy efficient sensor nodes has been monitored using trust and reputation systems.

The wireless sensor networks deals with two important aspects of sensor network formation. These two networks are 1) Flat sensor network 2) clustered sensor network. As the sensor nodes are in limited number the flat sensor network is simple, applicable and affordable. But when the system applications need more number of sensor nodes, we are in the need to migrate for clustered sensor network. The sensor nodes are clustered into groups. Every cluster should have the cluster head. It acts as an aggregate node processed for decision making using Iterative Filtering Algorithm(IFA) to find the trustworthiness of the individual sensor nodes.

The lifetime of the sensor node can be improved using sleep-awake technique. So that individual sensor nodes are pre-checked before the process of data aggregation. It predicts all the sensors that are

reliable. Collision attack is identified in the techniques of trust and reputation systems. It balances the traffic load throughout the network.

II. RELATED WORK

A wireless network consisting of a large number of small sensors. In hierarchical routing, the entire network is divided into several clusters. Each cluster consists of some source nodes and a cluster head. Sensor nodes, referred as source nodes, can gather information from the monitoring region and send the sensing information to their corresponding cluster head. The cluster head is elected from all the sensor nodes in a cluster according to some criteria, and is responsible for collecting sensing data from source nodes. Sensors communicate information only to cluster heads and then the cluster heads communicate the aggregated information to the processing center, may save energy. After receiving data from source nodes, the cluster head also performs data aggregation to reduce the data size before sending data to the sink, which further reduces the power expended for data transfer [1].

The sleep scheduling scheme is also incorporated in the protocol. The scheme is useful in saving energy. Saving energy leads to expansion of network lifetime. Intelligent sleep scheduling scheme along with the cluster of cluster heads protocol is a best way to improve the energy efficiency of the network. Improving the energy efficiency will ultimately increase the network lifetime. For communication to takes place, source and destination is chosen for transferring the data. Calculation of threshold value is done for differentiating the available nodes. Nodes are then differentiated as per the calculated threshold value i.e. mean energy. Accordingly flags are set as 0 and 1. Flag 0 is for sleep nodes and flag 1 for active nodes [2].

Trust and reputation systems have a significant role in supporting operation of a wide range of distributed systems. A trustworthiness assessment at any given moment represents an aggregate of the behavior of the participants up to that moment and has to be robust in the presence of various types of faults and malicious behavior. The main target of malicious attackers are aggregation algorithms of trust and reputation systems. WSNs will be able to afford hardware which can implement more sophisticated data aggregation and trust assessment algorithms [3].

Compressive sensing has witnessed an increased interest recently courtesy high demand for fast, efficient and in-expensive signal processing algorithms, applications and devices the compressive sensing paradigm, banking on finding sparse solutions to underdetermined linear systems, can reconstruct the signals CS combines the sampling and compression into one step by measuring minimum samples that contain maximum information about the signal this eliminates the need to acquire and store large number of samples only to drop most of them because of their minimal value [4].

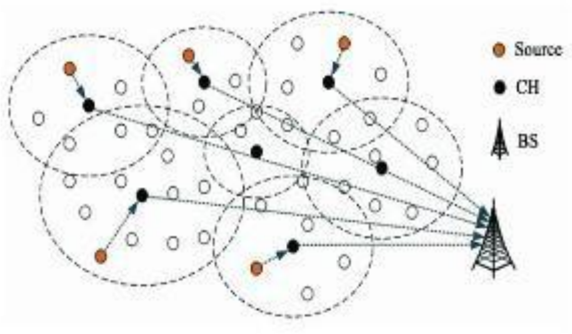
The cluster based routing algorithm to extend the lifetime of the networks and to maintain a balanced energy consumption of nodes. The clustering scheme in a wireless sensor network enables an aggregate data of cluster member nodes at the cluster head and can easily provide the network scalability due to node increase. In each of the many clusters in this network resides a cluster head which collects data from sensor nodes within its group, completes data aggregation, and sends them to the sink node of the network. Such data aggregation can reduce the consumption of node energy and the transmission delay as compared to multi-hop routing protocols. The performance of the proposed protocol has been examined and evaluated with the NS-2 simulator [5].

An efficient power saving scheme and corresponding algorithm must be developed and designed in order to provide reasonable energy consumption and to improve the network lifetime for wireless sensor network systems. In this article, we propose a clustering algorithm to provide efficient energy consumption in such networks. The main idea of this article is to reduce data transmission distance of sensor nodes in wireless sensor networks by using the uniform cluster concepts. In order to make an ideal distribution for sensor node clusters, we calculate the average distance between the sensor nodes and take into account the residual energy for selecting the appropriate cluster head nodes. The lifetime of wireless sensor networks is extended by using the uniform cluster location and balancing the network loading among the clusters [6].

We analyze the sleep & wakeup approach, in order to avoid the hot spot (WLAN) problem, which aims to increase the network lifetime using energy conservation as well as increasing packet delivery ratio (PDR). In this technique, C-H (cluster-head) has been selected based on energy level & Base-Station distance. Using this technique, we can improve the energy conservation & PDR up to 63%, when compare to that of FCA (fuzzy clustering algorithm) according to their parameters of FND (First Node Dead) and HNA (Half of the Node Alive) parameter

the sleep & wakeup approach is better and energy parameters [8].

III. SYSTEM MODEL



IV. CLONE DETECTION MECHANISM:

Trust and Reputation Systems are used to find the trustworthiness. Iterative filtering algorithm is used to identify the attacker. The iterative method for trust and reputation system can be monitor by using sniffers management and improve the energy efficient. The working mechanism of iterative filtering algorithm was proposed and the scheme of IF is robust in filtering out the peers who provide unreliable data ratings. Finally the Iterative method for Trust and Reputation Management referred as ITRM.

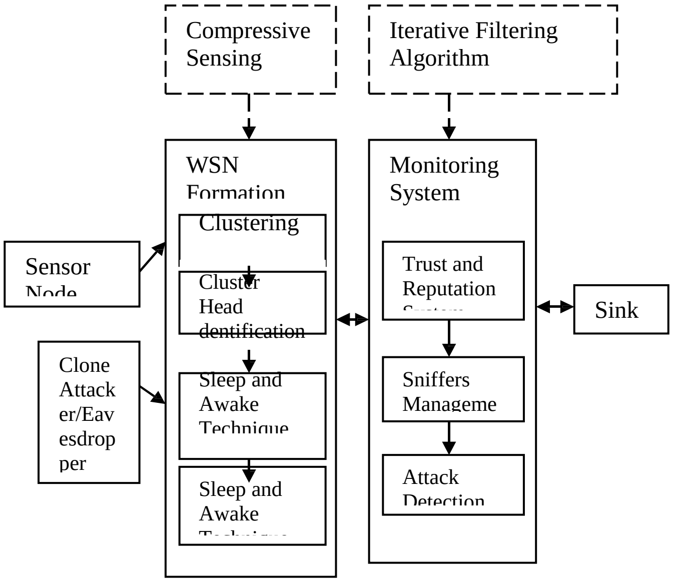
V. LIFETIME IMPROVEMENT:

Compressive sensing (CS) can reduce the number of data transmissions and balance the traffic load throughout networks. Compressed sensing (also known as compressive sensing, compressive sampling, or sparse sampling) is a signal processing technique for efficiently acquiring and reconstructing a signal, by finding solutions to underdetermined linear systems. This is based on the principle that, through optimization, the sparsity of a signal can be exploited to recover it from far fewer samples than required by the Shannon-Nyquist sampling theorem. There are two conditions under which recovery is possible. The first one is sparsity which requires the signal to be sparse in some domain. The second one is incoherence which is applied through the isometric property which is sufficient for sparse signals.

VI. SLEEP AWAKE SCHEDULING:

The Sleep Awake scheduling scheme is useful in saving energy. Saving energy leads to expansion of network lifetime. The lifetime of the sensor node can be improved using sleep-awake technique. So that individual sensor nodes are pre-checked before the process of data aggregation. It predicts all the sensors that are reliable. Sleep Awake technique are implemented in this system, While going for a switch from active to sleep state, and then from sleep to active state, the condition to be checked is that the energy it consumes for the switch should be low when compared with the energy it consumes when it is always in the active state.

SYSTEM ARCHITECTURE


Compressive Sensing
Iterative Filtering Algorithm
WSN Formation
Clustering
Cluster Head dentification
Sleep and Awake Technique
Sleep and Awake Technique
Sensor Node
Clone Attack er/Eav esdrop per
Monitoring System
Trust and Reputation System
Sniffers Manageme
Attack Detection
Sink

VII. LIST OF EXPERIMENTAL SETUP

- Sensor Network Formation
- Sensor Node Clustering
- Eavesdropper Attack
- Attack Detection and Energy efficiency Maintenance

VIII. SENSOR NETWORK FORMATION:

The sensor source nodes are fixed in hostile environments too. Thus the fixed sensor source nodes sense the signals which would be needed and sensed signals are collected to the sensor reader for decision making. The multiple source nodes may also for some of the domains based on the applications. The data gathering from the multiple source nodes are complex when the number of nodes may increased. The major thing is to provide the reduce number of transmissions in both inter and intra cluster sensor networks. However, the aggregate nodes are used to gather the some of the sensor sources and then it sends that data signal to the reader for decision making. In that it needs the trustworthiness and robustness for the data aggregation.

IX. SENSOR NODE CLUSTERING:

In this section, we present the centralized clustering algorithm called Compressive Sensing. Given the network G, our algorithm has two major steps: 1) select C CHs from the set V of N sensor nodes and divide the sensor nodes into C clusters and construct a

backbone routing tree that connects all CHs to the sink. The k-median problem is NP-hard. A lot of heuristic algorithms have been proposed to solve the k-median problem. We adopt an efficient method that iteratively closes to the near-optimal solution. Our algorithm starts from an initial set of CHs, which is randomly selected. At each iteration, the algorithm proceeds following steps:
Connect sensor nodes to their closest CHs. Ties break arbitrarily. For each cluster, choose a new CH, such that the sum of the distances from all nodes in this cluster to the new CH is minimized.

X. EAVESDROPPER ATTACK:

The Cluster based network topology may construct the wireless sensor network for secure and energy efficient data aggregation. Thus the sensor nodes formed as a cluster. The cluster gathers all the signals from the various sensors in the cluster. The cluster head or data aggregator compute and resend the signals to the sink. There is no possible to attack the cluster head to make the false data sending. The individual node attacked and the nodes send the false data signal to the aggregator. From the false data aggregation, the decision making may processes. This type of attacks referred as collusion attacks in secure data aggregation.

XI. ATTACK DETECTION AND ENERGY EFFICIENT MAINTENANCE:

Trust and Reputation Systems are used to find the trustworthiness. Iterative filtering algorithm is used to identify the attacker. The iterative method for trust and reputation system can be monitor by using sniffers management and improve the energy efficient. Sleep and Awake technique is used to and increase the lifetime of the sensor nodes. The adjacent pairs are created and the sleep and awake technique implemented by this mechanism.

XII. CONCLUSION

In this paper we have proposed energy efficient clone detection using Iterative Filtering Algorithm and to increase the network lifetime using Sleep- Awake Technique. Compressive Sensing can balance the network traffic. To provide the clustered environment for data aggregation in wireless sensor network and make energy efficient sensor nodes with energy monitoring.

REFERENCES

[1] Anju, Sandeep Tayal “Energy Efficient Clustering in Wireless Sensor Network: A Review”2012

[2] Anuja A. Pagrut, Archana R. Raut “An Adaptive Sleep Scheduling Algorithm for Improved Routing in Wireless Sensor Network”2016

[3] G.Gomathi ,C.Yalini, T.K. Revathi “Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Security Threats”October 2014

[4] Saad Qaisar, Rana Muhammad Bilal, Wafa Iqbal, Muqaddas Naureen and Sungyoung Lee ”Compressive Sensing: From Theory to Applications,
A Survey”2013

[5] Uk-Pyo Han, Sang-Eon Park, Seung-Nam Kim, Young-Jun Chung “An Enhanced Cluster Based Routing Algorithm for Wireless Sensor Networks”2006

[6] D.Suresh, K.Selvakumar “Improving Network Lifetime and Reducing Energy Consumption in Wireless Sensor Network”2014

[7] Dr.M.Senthil, Dr.P.Sivakumar, T.C.Indhumathi ”Sleep Wakeup Technique based Clustering Protocol Performance Evaluation in Wireless Sensor Network”