ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 10, Issue, 05(C), pp. 32310-32314, May, 2019

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

A LITERATURE SURVEY ON SECURING NODE CAPTURE ATTACKS FOR HIERARCHICAL DATA AGGREGATION IN STATIC CLUSTER HEAD BASED WSN'S

K.Suriya and Mr.R.Karuna Moorth

Erode Sengunthar Engineering College,Erode

DOI: http://dx.doi.org/10.24327/ijrsr.2019.1005.3442

ARTICLE INFO

Article History:
Received 15th February, 2019
Received in revised form 7th March, 2019
Accepted 13th April, 2019
Published online 28th May, 2019

Key Words:

The real world application is mainly depends on Wireless Sensor networks (WSNs).

ABSTRACT

The real world application is mainly depends on Wireless Sensor networks (WSNs).The Data Collection Scheme is the major task used in WSN. In Earlier system The Velocity Energy-efficient and Link-aware Cluster-Tree (VELCET) scheme and dynamic clustering scheme is used for data collection in WSNs. The VELCET scheme failed to mitigate the problems of coverage distance, mobility, delay, traffic, tree intensity and end-to-end connection. On the other hand the VELCT select the cluster head statically. Then the dynamic clustering used to select the cluster head dynamically. At a certain amount of time, the clustering changes the cluster head dynamically. The Data Collection Tree (DCT) used to collect the information and tree formation is initiated. The dynamic cluster head is formed based on the tree formation formed in the cluster. The Proposed scheme minimizes the energy exploitation, reduces the end-to-end delay and traffic in cluster head in WSNs by effective usage of the DCT. Adding security to dynamic protocols is challenging because they dynamically, randomly, and periodically rearrange the network's clusters and data links. Therefore, providing steady long-lasting node-to-node trust Relationships and common key distributions are inadequate for dynamic CH protocols. The proposed system uses the concept named SNCAHDA (Securing Node Capture Attacks for Hierarchical Data Aggregation). The key idea of SNCAHDA is it does not changes from static CH to dynamic CH rather it maintain the processing center for each static CH. In case of failure of static CH the processing center acts as a backup device and provides the data without network or node failure. This scheme also authenticate the encrypted sensed data, by applying digital signatures to message packets, which are efficient in communication and applying the key management for security.

INTRODUCTION

A wireless sensor network (WSN) is a network system comprised of spatially distributed devices using wireless sensor nodes to monitor physical or environmental conditions, such as sound, temperature, and motion. The individual nodes are capable of sensing their environments, processing the information data locally, and sending data to one or more collection points in a WSN Efficient data transmission is one of the most important issues for WSNs. Meanwhile, many WSNs are deployed in harsh, neglected, and often adversarial physical environments for certain applications, such as military domains and sensing tasks with trustless surroundings.

Cluster Based Wireless Sensor Network

Clustering protocols are often used in sensor networks. In a cluster-based WSN (CWSN), every cluster has a leader sensor node, regarded as cluster head (CH). A CH aggregates the data collected by the leaf nodes (non-CH sensor nodes) in its cluster, and sends the aggregation to the base station (BS). A CWSN consisting of a fixed BS and a large number of wireless sensor nodes, which are homogeneous in functionalities and capabilities. We assume that the BS is always reliable, i.e., the BS is a trusted authority (TA). Meanwhile, the sensor nodes may be compromised by attackers, and the data transmission may be interrupted from attacks on wireless channel.In a CWSN, sensor nodes are grouped into clusters, and each cluster has a CH sensornode, which is elected autonomously. Leaf (non-CH) sensornodes join a cluster depending on the receiving signalstrength and transmit the sensed data to the BS via CHs tosave energy. The CHs perform data fusion, and transmitdata to the BS directly with comparatively high energy. Inaddition, we assume that all sensor nodes and the BS aretime synchronized with symmetric radio channels, nodesare distributed randomly, and their energy is constrained. In CWSNs, data sensing, processing, and transmission consume energy of sensor nodes. The cost of data transmission is much more expensive than that of data processing.

Corresponding author:* **K.Suriya
Department of Botany, School of Sciences, Gujarat University Ahmedabad

Purpose

The main purpose of security requirements is to identify the information and resource from attacks and misbehavior. Symmetric key cryptography is power consumption in sensor nodes. Open research issues are high speed and low energy cost. In this efficient and flexible key distribution are to be design. There are many routing techniques are been designed for WSNs. Some networks are been design security as a goal.

Product Scope

The main aim of the proposed work is to provide security for the data in wireless network as the data is to be passed through wireless channel. Therefore, two security protocols SET-IBS and SNCAHDA are proposed. With the help of these two protocols energy consumption can also be reduced as shown in the simulation results.

Literature Survey

Leach Protocol

In a cluster-based WSN (CWSN), every cluster has a leader sensor node, regarded as cluster head (CH). A CH aggregates the data collected by the leaf nodes (non-CH sensor nodes) in its cluster, and sends the aggregation to the base station (BS). The low-energy adaptive clustering hierarchy (LEACH) protocol presented is a widely known and effective one to reduce and balance the total energy consumption for CWSNs. To prevent quick energy consumption of the set of CHs, LEACH randomly rotates CHs among all sensors nodes in the network, in rounds. LEACH achieves improvements in terms of network lifetime.

Secleach-(Security Leach)

This paper investigates the problem of adding security to hierarchical/cluster-based sensor networks where clusters are formed dynamically and periodically, such as LEACH. For this purpose, random key pre distribution, of flat networks, can be used to secure communications in CWNS. The main advantage of this scheme was security is concerned.

Gsleach-(Grid-Based Secure Leach)

The GS-LEACH (grid-based secure LEACH) protocol uses pre deployment key distribution using prior knowledge of the deployment area. The main advantage of this method is The GS-LEACH protocol is more energy efficient than any of the secure flavors of LEACH also GS-LEACH provides a longer network lifetime compared to the other flavors of LEACH.

Rleach-Routing Leach

In this paper, we investigate adding security to cluster-based routing protocols for wireless sensor networks which consisted of sensor nodes with severely limited resources, and introduce a security solution for LEACH, a protocol in which the clusters are formed dynamically and periodically. Our solution uses improved random pair-wise keys (RPK) scheme, an optimized security scheme that relies on symmetric-key methods. The main advantage of this method is RLEACH Is Lightweight and Preserves the Core of the Original LEACH and also Security of RLEACH Has Been Improved. This method consumes Less Energy.

Cluster Formation

Sensor node is deployed in wireless sensor network that provides physical environment that roduce similar data in close by sensor node and transmitting such type of data is easy. The facts are encourage using some kind of grouping of sensor nodes such that group of sensor node can be combine or compress with each data together and transmit only the relevant data. This group of sensor nodes in a densely deployed large scale sensor node is known as clustering. The way to combine the data and define the data belonging to a single cluster called data aggregation. Issues of clustering in wireless sensor network have a major cause in a network, it means user can put all the full nodes, in term of energy in the network it can behave like cluster head and simple node in a cluster work as CM.

Data Aggregation Techniques Leach

LEACH (low-energy adaptive clustering hierarchy) is a cluster based protocol to minimize the energy, and reduce the transmission towards to the Base station. It reduces the network traffic and addition to this channel. LEACH has motivated the design of several other protocols and tries to improve the CH selection process. These Protocols basically differ on the application and network architecture used in the design. Number of cluster based routing protocols proposed in survey for WSNs. LEACH gives the better energy consumption and performance compare to the large-scale WSNs, but it also increases the overhead to maintain. It is one of the hierarchical routing approaches for WSNs.

It is a cluster based protocol that utilizes randomized rotation of local base station to evenly distribute the energy load among the sensors in the network. The working of LEACH is broken up into rounds of actions. The clusters are being created and each node decides whether or not to become a CH for the current round. This decision is based on the suggested percentage of CHs for the network and the number of times the node has been used. The nodes are chosen based on choosing a random number between 0 and 1 LEACH-C (leach-centralized) protocol is an enhancement of LEACH. It uses a clustering algorithm to elect CH and same steady –state phase like as LEACH. During the set-up phase of LEACH-C, each node sends the information about it to BS such as current location and residual energy level.

To maintain the clusters, the BS needs to ensure that the energy load is distributed among all the nodes. For this, BS computes the average node energy, and determines the nodes have low energy. The nodes have energy above or average level can be select for the CHs for the current round. Once the CHs and other clusters are found, the Base Station broadcast a message that obtains the CH ID for each node. If the CH ID matches its own ID, the node is a CH, otherwise the node uses the TDMA slot for data transmission and goes sleep time to transmit data.

LEAC Huses distributed algorithm and offers no guarantee to the number of CHs. LEACH-C protocol can produce better performance by dispersing the CHs throughout the network.

CM is a clustering-based and time-driven protocol which minimizes energy dissipation for data gathering with mobile

sensor nodes. In this protocol, the cluster formation is done based on node's mobility. The sensor node uses the information obtained from GPS device to estimate its distances from all other CHs. Clustering-based data gathering protocol works in rounds. Christo Ananth *et al*. discussed about a method, Wireless sensor networks utilize large numbers of wireless sensor nodes to collect information from their sensing terrain. Wireless sensor nodes are battery-powered devices. Energy saving is always crucial to the lifetime of a wireless sensor network. Recently, many algorithms are proposed to tackle the energy saving problem in wireless sensor networks. There are strong needs to develop wireless sensor networks algorithms with optimization priorities biased to aspects besides energy saving. In this project, a delay-aware data collection network structure for wireless sensor networks is proposed based on Multi hop Cluster Network. The objective of the proposed network structure is to determine delays in the data collection processes. The path with minimized delay through which the data can be transmitted from source to destination is also determined.

Objective of the Project

1. The specific objective of the project is to create the secure and efficient data transmission for cluster-based WSNs (CWSNs), where the clusters are formed statically and periodically.
2. Need to Implement the SNCAHDA protocols with respect to the security and failure requirements.
3. The proposed SNCAHDA protocols need to consume energy faster than LEACH protocol because of the communication and computational overhead for security,
4. The proposed SNCAHDA need to achieve a better balance of energy consumption than that of Sec LEACH protocol.

- ✓ SNCAHDA protocols need to provide
- ✓ Solutions to passive attacks on wireless channel
- ✓ Solutions to active attacks on wireless channel.
- ✓ Solutions to node compromising attacks.

Existing System

Leach Protocols

In a cluster-based WSN (CWSN), every cluster has a leader sensor node, regarded as cluster head (CH). A CH aggregates the data collected by the leaf nodes (non-CH sensor nodes) in its cluster, and sends the aggregation to the base station (BS). The low-energy adaptive clustering hierarchy (LEACH) protocol presented is a widely known and effective one to reduce and balance the total energy consumption for CWSNs.

Velcet

The Velocity Energy-efficient and Link-aware Cluster-Tree (VELCT) scheme for data collection in WSNs which failed to mitigate the problems of coverage distance, mobility, delay, traffic, tree intensity and end-to-end connection. The VELCT select the cluster head statically.

Dynamic Cluster

The dynamic clustering used to select the cluster head dynamically. At a certain amount of time, the clustering changes the cluster head dynamically. The Data Collection Tree (DCT) used to collect the information and tree formation is initiated. The dynamic cluster head is formed based on the tree formation formed in the cluster. In this system the dynamic clustering used to group the nodes. It can be selected based upon the nodes placed in the WSN. The nodes are located anywhere in the network. The important way to group the nodes based on the cluster form in the network. After form the cluster, the tree formation of network has been initiated.

The tree formation is initiated with the help of performing tree related techniques such as Breadth first Search, Depth first search and others. Each technique consists of two phases: Dynamic set-up phase and Dynamic steady-state phase. Dynamic Set-up Phase divided into Intra-Tree Formation and Cluster Tree Selection. Dynamic Steady state Phase includes Transmission of data.

Disadvantages of Existing System

Adding security to dynamic protocols is challenging because they dynamically, randomly, and periodically rearrange the network's clusters and data links. Therefore, providing steady long-lasting node-to-node trust Relationships and common key distributions are inadequate for dynamic CH protocols (most existing solutions are provided for distributed WSNs, but not for CWSNs).

There are some secure data transmission protocols based on LEACH-like protocols, such as Sec LEACH, GS-LEACH, and RLEACH. Most of them, however, apply the symmetric key management for security, which suffers from so-called orphan node problem.

- ✓ Since the more CHs elected by them, so the more overall energy consumed for the network.
- ✓ The orphan node problem increases the overhead of transmission and system energy consumption by raising the number of CHs.
- ✓ Even in the case that a sensor node does share a pair wise key with a distant CH but not a nearby CH, it requires comparatively high energy to transmit data to the distant CH.

Proposed System

In Existing System, the aggregate data to be transmitted via sensor nodes, a security threat is originate by any node. So, that time hacker achieves full control over a dynamic CH node through direct physical path in wireless sensor network. It makes to data loss and risk of data confidentially. In this while changing from static to dynamic the CH are exposed to maximum failures. Sensor nodes which make use of the broadcast communication pattern and have severe bandwidth restraint. Sensor nodes have inadequate amount of resources.
In Proposed System the distinct Structure and Securing Node Capture Attacks for Hierarchical Data Aggregation (SNCAHDA) is used to avoid data loss. Initially network is separated into different clusters each cluster is headed by an aggregator AND processing center and directed connected to sink. So, this idea basically dispersed data processing measures to save the energy.

Advantages of Proposed System

It proposed the Protocol offers

A better Secure Communication,

1. Secure data aggregation,
2. Confidentiality and
3. Resilience against node capture and
4. Replication attacks using reduced resources.

Modules

1. Wireless Sensor Network
2. Hierarchical secure data aggregation
3. Node capture attacks
4. Slicing technique and Performance Metrics
5. Simulation Result

Wireless Sensor Network

In this module, Sensor networks consist of numerous low cost, little devices and are in nature self-organizing ad hoc systems. The job of the sensor network is to monitor the physical environment, gather and transmit the information to other sink nodes. Generally, radio transmission ranges for the sensor networks are in the orders of the magnitude that is lesser that of the geographical scope of the unbroken network. Hence, the transmission of data is done from hop-by-hop to the sink in a multi-hop manner. Reducing the amount of data to be relayed thereby reduces the consumption of energy in the network.

Hierarchical Secure Data Aggregation

In this module, combine the data from different sources, redirect it with the removal of the redundancy and thereby reducing the number of transmissions and also saves energy. The inbuilt redundancy in the raw data gathered from various sensors can be banned by the in-network data aggregation. The copy of aggregated data should be stored into the processing center.

Data Confidentiality

In particular, the fundamental security issue is the data privacy that protects the transmitted data which is sensitive from passive attacks like eavesdropping. The significance of the data confidentiality is in the hostile environment, where the wireless channel is more prone to eavesdropping. Though cryptography provides plenty of methods, such as the process related to complicated encryption and decryption, like modular multiplication of large numbers in public key based on cryptosystems, utilizes the sensor's power speedily.

Data Integrity

It avoids the modification of the last aggregation value by the negotiating source nodes or aggregator nodes. Sensor nodes can be without difficulty compromised because of the lack of the expensive tampering-resistant hardware. The otherwise hardware that has been used may not be reliable at times. A compromised message is able to modify, forge and discard the messages.

Node Capture Attacks

In this module, the process of getting hold of the sensor node through a physical attack is termed as node capture attack. For example: uncovering the sensor and adding wires in any place. This attack essentially differs from getting hold of a sensor via certain software bug. Since sensors are typically supposed to operate the same software, specifically, the operating software which discovers the suitable bug permits the adversary to manage the entire sensor network. Distinctly, the node capture attacks can be set over a small segment of adequately large network.

There are two Types of node Captures Possible

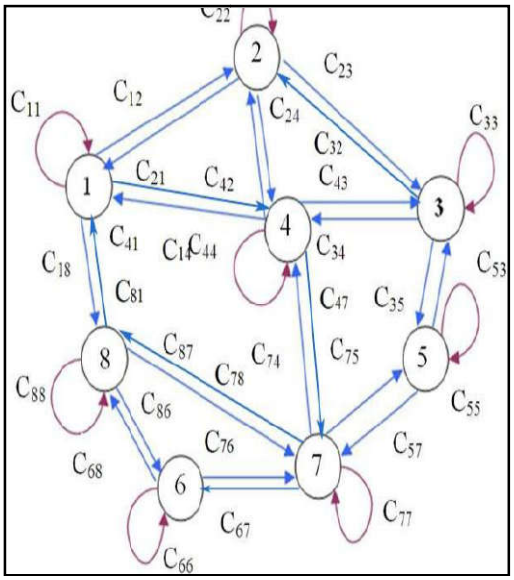
a. Random node capture
b. Selective node capture

Slicing Technique and Performance Metrics

The performance of Securing Node Capture Attacks for Hierarchical Data Aggregation in Wireless Sensor Networks (SNCAHDA) protocol is compared with our previous work Secure Authentication Technique for Data Aggregation (SATDA) protocol.

The Performance is Evaluated Mainly, According to the Following Metrics

1. Average end-to-end delay
2. Average Packet Delivery Ratio
3. Average Energy
4. Average Packet Loss
5. Throughput



CONCLUSION

In this paper, we have proposed Securing Node Capture Attacks for Hierarchical Data Aggregation in Wireless Sensor Networks through the processing center. During first round of data aggregation, the aggregator upon identifying the detecting nodes selects a set of nodes randomly and broadcast a unique value which contains their authentication keys, to the selected set of nodes. When any node within the set wants to send the data, it sends slices of data to other nodes in that set, encrypted with their respective authentication keys. Each receiving node decrypts, sums up the slices and sends the encrypted data to the aggregator. The aggregator aggregates and encrypts the data with the shared secret key of the sink and forwards it to the sink. In the second round of aggregation, the set of nodes is reselected with new set of authentication keys. By simulation results, we have shown that the proposed approach rectifies the security threat of node capture attacks in hierarchical data aggregation.

Future Enhancement

Future scope of it is to determine reducing the cost and power consumption which can be highly useful in the future. Our current analysis are based on a simple three cluster model, further systematic studies of more generalized multi-cluster networks are needed. Thus far we have concentrated on the homogeneous sensor networks with a single powerful processing center (sink). In our future work, we would rather focus on the heterogeneous wireless sensor networkswith multiple resource-rich actors for carrying out energy consuming tasks.

References

1. W. Heinemann, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Micro sensor Networks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660-670, Oct. 2002.
2. L.B. Oliveira *et al*., "SecLEACH-On the Security of Clustered Sensor Networks," Signal Processing, vol. 87, pp. 2882-2895, 2007.
3. P. Banerjee, D. Jacobson, and S. Lahiri, "Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks,"Proc. IEEE Sixth Int'l Symp. Network Computing and Applications (NCA), pp. 145-152, 2007.
4. K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," Proc. Fourth Int'l Conf. Wireless Comm 1-5, 2008.
5. Shamir, "Identity-Based Cryptosystems and Signature Schemes," Proc. Advances in Cryptology (CRYPTO), pp. 47-53,1985.
6. J. Liu *et al*., "Efficient Online/Offline Identity-Based Signature for Wireless Sensor Network," Int'l J. Information Security, vol. 9, no. 4, pp. 287-296, 2010.
7. Velmani Ramasamy and Kaarthick Balakrishnan, AnEfficient Cluster-Tree based Data Collection Scheme for Large Mobile Wireless Sensor Networks, IEEE Sensor Journal, Vol 15, No. 4, April 2015.
8. Akkaya K and Younis M, "A survey of routing protocols in wireless sensor networks," Elsevier Ad Hoc Network. 3/3, 2005, 325-349.
9. Mehdi Tarhani, Yousef S.Kavnin, Saman Siavoshi,"Scalability Energy Efficient Clustering hierarchy Protocol in WSN", IEEE Sensor journal, Vol 14, No. 11,November 2015.
10. Christo Ananth, T.Rashmi Anns, R.K.Shunmuga Priya, K.Mala, "Delay-Aware Data Collection Network Structure For WSN", International Journal of Advanced Research in
11. Biology, Ecology, Science and Technology (IJARBEST), Volume 1,Special Issue 2 - November 2015, pp.17-21
12. 11.X. Liu, "A survey on clustering routing protocols inwireless sensor networks", Sensorsvol. 12, no. 8, pp.11113-11153, 2012.

How to cite this article:

K.Suriya. *et al*.., 2019, A Literature Survey on Securing Node Capture Attacks for Hierarchical Data Aggregation in Static Cluster Head Based Wsn's. *Int J Recent Sci Res.* 10(05), pp. 32310-32314. DOI: http://dx.doi.org/10.24327/ijrsr.2019.1005.3442

****