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

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 9, Issue, 11(B), pp. 29586-29589, November, 2018

ISSN: 0976-3031

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

POWER PROFICIENT DATA AGGREGATION IN WIRELESS SENSOR NETWORKS

Mohamed Yacoab[1]., Mohemmed Sha[2] and Mohamed Mustaq Ahmed[3]

[1]MIIT, Chennai
[2]Prince Sattam Bin Abdulaziz University, KSA
[3]Edgeover Technologies, Chennai

DOI: http://dx.doi.org/10.24327/ijrsr.2018.0911.2888

ARTICLE INFO

Article History:

Received 4th August, 2018
Received in revised form 25th September, 2018
Accepted 18th October, 2018
Published online 28th November, 2018

Key Words:

Sensor Networks, Mobility, Data Gathering, Time Based Protocol , Polynomial Based Protocol

ABSTRACT

Wireless Sensor Networks (WSN) increases the lifetime and durability of the network by reducing the power consumption of the hops. The hops are grouped into clusters and a distinct hop is selected to be the Cluster Head (CH) that collects the data and process it. The Mobile Data Collector (MDC) is a special node in the sensor network to gather the data securely and stores in the base station or sink hops (BS). With the help of the tree network based administration and management scheme, three protocols are proposed and analyzed for a secured data collection. The analysis shows that these three protocols are not showing any impact on the compromised MDC, compromised CH and the replay messages. Simulation results deals with the energy consumed by the three protocols.

INTRODUCTION

The WSNs consist of sensor hops and a sink hop. The sink hop is also called as Base station (BS).In a WSN the data's are sensed and then transferred to the base station. The mobile agent known as Mobile Data Collector (MDC) collects the data in a network securely and reducing the power consumed by the nodes and store in a base station. The advantage of using the MDC is to minimize the energy consumption and also to improve the lifetime of the sensor network. By using MDC the data latency has improved means the time taken by the sensor data from the its generation time to time it lands in the base station. Instead of, the cluster head listening and transferring the data if MDC transfers the data latency improved and power consumption is also reduced. The beacon signal is transmitted by the MDC to the cluster head to collect the data securely. If the beacon signal transmitted by MDC is not authenticated, it will attempt the adversary attack. Major problem in the sensor network is the node compromise and thus solved. The node compromise includes MDC compromise and the CH compromise. The security issues provided in the research paper is to detect the malicious MDC, finding and Identifying replay messages and compromise of sensor hops. The three proposed protocols for the secured data collection in the WSNs are stated as 1) Time based Impression Procedure (TIP), 2) Polynomial Point Allotment Procedure (PPAP) and 3) Secret Allocation and Distribution Procedure (SADP) are designed according to the several assumptions and some considerations.

LITERATURE REVIEW

The research work has divided in to two sections. In the first phase, we discuss about the concept of mobile communication. In the second phase the existing work is discussed.

Mobility for Communication

The Mobile Data Collector is utilized for the applications such as information transfer, information gathering and other physical activities such as replacement of defective sensors. The primary idea of MDC was to connect the sparse sensor networks and then for a multiple MDC system for travelling straight line in a network was introduced. Then for avoiding the obstacle we used and also for reducing the data latency.

Protected Data Gathering

The mobile sink uses a certain path for communicating between the sink and to transfer the data. The mobile agent visits the hop for the data collection in the particular designated path.

Corresponding author:* **Mohamed Yacoab
MIIT, Chennai

Network Design model, adversary Model and notations

Network Design model

The network model is considered as the large scale homogeneous network requires high cost for communication, storage and other purpose. Due to the overheads associated in the network Design model a Hierarchical Sensor Network (HSN) is preferred and hence chosen to work on it. The network model consists of two nodes viz., Powerful high-end nodes (cluster head) and Low-end sensor nodes((SN-sensor)).
CHs are made more powerful with high speed computation, high speed Communication with other nodes, high-end energy and storing capability. The sensor node has the limited resources in the above mentioned. The SN-sensors receives the data and transmits it to CH for data aggregation. Using MDC the aggregated data are transferred to the base station. The MDC considered here is the special node moving in a monitoring area with high memory. This helps in Base Station for further processing.

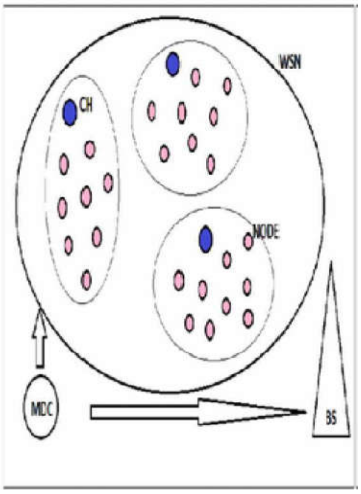

Fig 1 Sensor node arrangement

Adversary Model

An adversary which increases malicious MDC are Unauthorized access, Worm hole hello flood attack, Worm hole sink hole attack and Attack on precise motion.

Unauthorized access: This will have a duplicate MDC for collecting the data from the cluster head.

Worm hole hello flood attack: This will sense the beacon message and transmit to cluster head to collect the data and making it legitimate.

Worm hole sink whole attack: This is an attack by placing one malicious node in the fixed path and hearing the beacon message and making the cluster head to send the gathered data to the malevolent MDC.

Assault on precise motion: CHs are not inside the trusted MDCs way will transmit the information over that channel

Node Compromise attack: If a node is compromised it reveals all the cryptographic detail in a network.

Cluster-group arrangement and key administration scheme

Cluster formation

The cluster formation is done with the help of SN-sensors and with several keys assigned for the base station, MDC and CH. After the cluster formation, two phases are used for the network operation. Sensing phase and Data collection phase. In sensing phase the data's are sensed by the SN-sensor from the nodes and the cluster head aggregate the data after the SN-sensor senses the data. In data gathering phase the MDC visits the group-head node and the group head will authenticate MDC and transfer the data securely. The MDC then transmits the secured data to the sink hop. The proposed algorithm determines the number of MDC for the maximum coverage. This algorithm is mainly used for choosing the minimum number of MDC for a network.

Tree oriented Administration and Management Scheme

The tree is headed with the cluster head followed by the number of SN-sensors and those sensors followed by the small group of nodes called the subgroups. Cluster keys are defined to be at the root level and it is shared by all the hops in the sensor network. The intermediate keys are used for the sensors. The Common Cluster Head Key (CCHK) is used in between the cluster head for the secure communication.

Time based Impression Procedure (TIP)

The first process of the protocol is described as the sink hops to collect the accumulated node-data from the cluster head. The MDC networks travels in the sensor network observing area and gather the aggregated data from the cluster head and store it in the sink hops. The secure data gathering utilizes the tree oriented administration and management scheme and the Time based Stamp Protocols for data collection and data aggregation. This scheme not only identifies the malicious MDC but also avoid the replay attack. This TIP protocol is also for the authentication purpose. The CCHK key is known only to the cluster head only after the confirmation that the data transfer is secure. The time imprints belong to the message communication will enable the cluster head to find the replay messages. To overcome the key stealing, the CCHK key and the decryption key is to be changed often.

Polynomial Point Allotment Procedure (PPAP)

The Time based Stamp Protocol uses the period interval or identifying the echo messages. This will request the synchronization clock in between the Cluster Head and the sink nodes. Polynomial based Distribution Protocol is used to avoid the synchronization clock. This is done by sharing the polynomial points. This also uses refreshed keys for providing security to the network. The cluster formation and the tree oriented administration scheme are similar to Time based Stamp Protocol.

Secret Allocation and Distribution Procedure (SADP)

The concept and idea of Shamir's secret sharing scheme is used in the secret allocation and sharing protocol. This protocol is used for the security purpose because the TIP protocol is used for reducing the energy consumption.

Security Analysis

Security analysis plays a vital role in protect the node data in the sensor networks. The issues to be addressed are lying in the core are such as pointing and finding the malicious MDC, finding and Identifying the echo (replay)messages and hop compromise (CH and MDC).

Finding the Malicious MDC and Echo Messages

Malevolent MDC provides various kinds of assault; by means of collect the data from the cluster head. By means of TIP protocol, the malevolent MDC gets by eavesdropping. The common key visible to Cluster Head and the sink node is cluster head key (CCHK). So the message can't decrypt by another user.CH authenticate for the replay message gets fails, because each message carries a separate unique time stamp encoded with CCHK. By using PPSP protocol as the beacon message, it doesn't disclose the session key (SK).Without knowing SK; the malevolent MDC doesn't authenticate itself. By using SSP, the SK is encrypted. Because the key is only visible to Cluster Head and the sink hops. So malevolent MDC cannot able to validate by itself. The echo message to the CH gets fails, because every message carries unique time stamp encrypt with key.

Node Compromise

MDC Compromise

The aggregated data collected in the cluster head is encrypted by secret key sand the data is transferred to the MDC. The secret key is dynamic at random intervals the key is changed. To authenticate the MDC the beacon message are utilized. Hence, protocols are very strong to compromise MDC.

CH Compromise

In the first iteration, the group- head send the data to MDC; the sink hops (BS) periodically release the MDC to accumulate the data into the network. After visiting all the CH, the MDC stores the data to the sink hops. The time-interval taken to complete for one iteration of data collection and aggregation is called as round-trip time. After compromising a Cluster Head the hacker gathers all the information that contained in the node.

TIP protocol*:* The hacker obtains the CCHK; Cluster Head is compromised during the time period. By perception the CCHK and the beacon message the hacker is able to deploy a malevolent MDC. In order to avoid that the time interval for which the data transfer among the CH and MDC is secure and susceptible to attacks by the hacker.

PPAP protocol: In a specific instance, if the cluster head is compromised, then the hacker obtains the necessary information by eavesdropping. So, in order to compute the session key for the compromised node the hacker has to spend some time to evaluate.

SADP protocol: The hacker gathers the sensed data by compromising a cluster head. To deploy a malevolent hop, the hacker calculates the secret key. The beacon message is generated for a particular Cluster Head to take the essential data message that will visit the compromised cluster head.

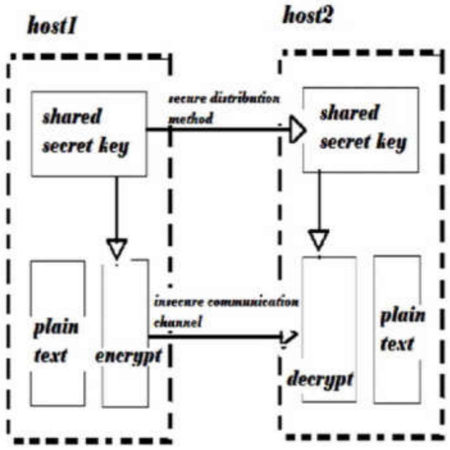

Fig 2 Cryptographic process arrangement

Performance Analysis

The performance analysis is the calculated based on the protocol factors with respect to data Communication, Computation Storage and energy efficiency.

Storage

In a sensor network the storage is intended to specify the vital data such as sensor networks, cluster head, mobile data collector and the intermediate nodes used in data collection and in data gathering. Moreover we need to specify further storage requirement for the encrypted key and other data of the nodes used in the sensor network.

Communication

In order to complete a validation and handover the data between Cluster Head and the MDC, number of messages are be exchanged between them. In TIP and PPSP, the number of message is used to validate the MDC. After this, to swap the encrypted node data between the CH and MDC a distinct message is exchanged. In SADP, the MDC directs a beacon communication to Cluster Head, upon reception of the communication message the CH directs the ID to the MDC.

Computation

Computations are carried out to validate the MDC and the details about the transmission the data. The TIP and PPAP protocol execute only cryptographic operation and a hash function to validate the mobile data collector and sends the data. In SADP, the Cluster Head does a cryptographic process and a single hash function to validate the mobile data collector. To send the node data the Cluster Head executes an encryption process and MDC performs a encryption and decryption for verification.

Energy Analysis

On the contrary, the energy utilization of the sensor nodes is simulated by using TIP, PPAP, and SADP protocols. The power utilization of TIP is increasingly stabilizing, while in PPAP and SADP procedures are surges in exponential fashion. In order to maintain the further security delivered by PPAP and SASP procedures a vital greater energy is essential.

Simulation Setup

Contents	Sample Values
nodes	**25**
area	350 X 350
MAC addr.	802.11
Simulation Time	40 sec
type of Source	CBR
Packet size	512
Transmit Power	0.561 w
battery Power	0.3696 w
battery Power in idle	0.036 w
Energy at initial stage	90.1 J
Transmission Range	705m
Total of sink hops	1
Total number of sources	6
Total number of data collector hops	10
Node values	Multiples of 4

Performance factors

The performance of Power Efficient Data Collector In Wireless Sensor Network is compared with LOW-END AND HIGH-END sensors in the network. The performance is assessed with the following criteria.

***End-to-end Delay Average**:* The delay is averaged over all current data packs from the initial sources to the final destinations.

***Packet Delivery Ratio**:* Ratio between the total numbers of data packets received over total number of data packets transmitted.

***Consumption of Energy**:* energy spent by all the hops in transfer, getting and dispatching data operations

The simulation results are presented in the next section.

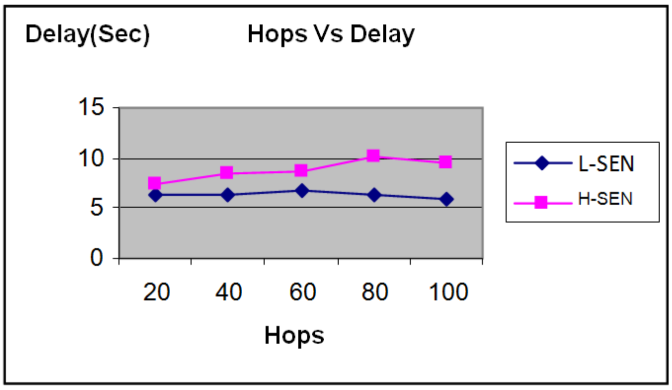

Fig 3 Hops Vs Delay

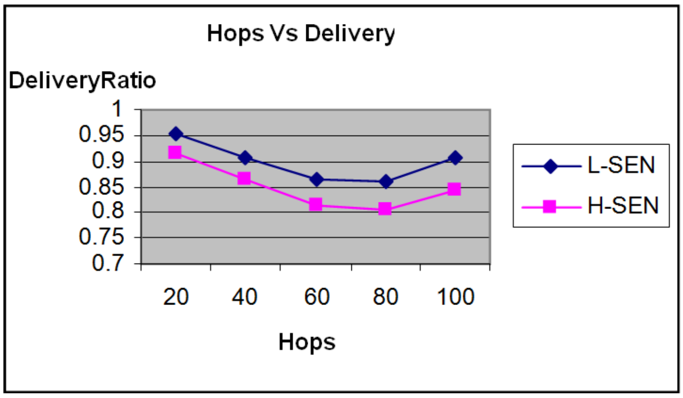

Fig 4 Hops Vs Delivery Ratio

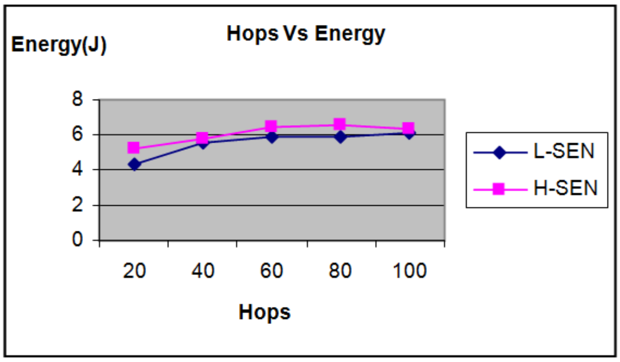

Fig 5 Hops Vs Energy

Analysis of Proposed Protocols

The different protocol conventions discussed in the past segments are utilized for secure information accumulation and conglomeration. The protocol convention is intended to suit to work as for a sort of utilization and execution. This analysis shows that CH compromise compared to TIP and SADP. SADP protocol requires message to be swapped. As an outcome, a polynomial operation is to organize a malevolent MDC. PPAP protocol needs a communication message "k" to be swapped and perform polynomial evolution process. TIP protocol replacing a distinct message and compromising a CH that will able to organize malevolent MDC for data collection.

CONCLUSION

Thus the power consumed by the three protocols was analyzed and the graph is shown. In clustered wireless sensor network, the important technique is used to increase the network life time. The data is collected in a secured way with the help of mobile data collector (MDC) and the three protocols. The protocols are constructed under tree based administration and management scheme. That protocol provides some vital sensor node security issues like malevolent MDC and echo (replay) communications messages. The study shows that planned protocols deliver atmost security against the attack sensor node.

References

1. Chen.: 'Data distribution based on mobile agent in WSN'. Proc. IEEE LCN 2005
2. Ma, M., Yang, Y.: 'SenCar: an energy-efficient data gathering mechanism for large-scale multi-hop sensor networks', IEEE Trans Parallel Distrib. Syst., 2007
3. Pornima, Amberker: 'Tree-based key mgmt. scheme for varied sensor networks'. IEEE Intl .Conf. on Networks
4. Poornima, Amberker, 'Agent based secure data collection in heterogeneous sensor networks'. Proc. Second Int. Conf. on Machine Learning and Computing (ICMLC 2010).
5. Qi, H., Xu, Y., Wang, X.: 'Mobile agent based collaborative signal and information processing in sensor networks', Proc. IEEE, 2003
6. Rasheed, A., Mahapatra, R.: 'Secure data collection scheme in wsn with mobile sink'. Proc. of Seventh IEEE Int. Sym. on Network Comp. Appls, 2008.
7. Shah, R., Roy, S., Jain, S., Brunette, W.: 'Data MULEs: modeling a three-tier architecture for sparse sensor networks'. Proc. IEEE Workshop on Sensor Network Protocols and Applications
8. Zhou, L., Ni, J., Ravishankar, C.V.: 'Supporting secure communication and data collection in mobile sensor networks'. Proc. 25th IEEE Int. Conf. on Computer Communications