IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 37-40
www.iosrjournals.org

A Paper On Cluster-based secure data aggregation in networks.

Sheetal Chate

(RSCOE, University of Pune, Pune, Maharashtra India)

Abstract: *Sensor networks are collection of sensor nodes which co-operatively send detected information to base station. As sensor nodes are battery driven, a efficient usage of power is essential with a specific end goal to utilize systems for long length of time consequently it is expected to reduce data traffic inside sensor networks, reduce amount of data that need to send to base station. The primary objective of data aggregation algorithms is to gather and aggregate data in an energy efficient manner so that network lifetime is enhanced. One such approach is data aggregation which attractive method of data gathering in distributed system architectures and dynamic access via wireless connectivity[5]. Wireless sensor networks have limited computational power and limited memory and battery power, this leads to increased complexity for application developers and often results in applications that are closely coupled with network protocols. In this paper, a data aggregation framework on networks is presented. The framework works as a middleware for aggregating data measured by a number of nodes within a network.*

***Keywords*:** *Data aggregation algorithm, Sensor network, WSN.*

I. Introduction

Sensor Networks: The remote sensor system is impromptu system. It comprises little light weighted remote hubs called sensor hubs, sent in physical or natural condition. Also, it quantified physical parameters, for example, sound, weight, temperature, and dampness. These sensor nodes conveyed in extensive or thousand numbers and team up to shape a specially appointed system fit for answering to information gathering sink (base station). Remote sensor system have different applications like territory observing, building checking, wellbeing checking, military survivallance and target following. With development in innovation, sensor systems made out of little and cost effective detecting gadgets outfitted with remote radio handset for environment observing have gotten to be feasible. The key advantage of utilizing these little devices to monitor the environment is that it does not require infrastructure, for example, electric mains for force supply and wired lines for Internet associations with gather information, nor need human collaboration while sending. These sensor hubs can screen nature by gathering data from their surroundings, and work agreeably to send the information to a base station, or sink, for examination [3].A sensor node that creates information, in view of its detecting systems perception and transmit detected information bundle to the base station (sink). This procedure essentially coordinate transmission since the base station may find extremely far from sensor hubs needs [6]. More vitality to transmit information over long separations with the goal that a superior method is to have fewer nodes sends information to the base station. These hubs called aggregator hubs and procedures called information conglomeration in remote sensor system.

II. Literature Survey

2.1) ‘Data aggregation in wireless sensor network’
AUTHORS: Patil, N.S., Patil, P.R.

Sensor networks are collection of sensor hubs which co- operatively send detected information to base station. As sensor hubs are battery driven, a productive usage of force is fundamental so as to utilize systems for long length of time consequently The principle objective of information collection calculations is to assemble and total information in a vitality productive way so that system lifetime is improved. In this paper, an information conglomeration structure on remote sensor systems is displayed. The structure fills in as a middleware for collecting information measured by various hubs inside of a system. The point of the proposed work is to look at the execution of TAG as far as vitality proficiency in examination with and without information total in remote sensor systems and to evaluate the convention's suitability in a domain where asset are restricted.

2.2) 'Secure data aggregation in wireless sensor networks.
AUTHORS: Roy, S., Conti, M., Setia, S., Jajodia, S.

In a huge sensor network, in-system information total altogether decreases the measure of correspondence and vitality utilization. In any case, this collection system does not address the issue of false subtotal qualities contributed by traded off hubs bringing about extensive lapses in the total figured at the base station, which is the root hub in the accumulation order. This is a critical issue since sensor systems are exceptionally helpless against hub bargains because of the unattended way of sensor hubs and the absence of alter safe equipment. In this paper, Exhaustive hypothetical examination and broad recreation study demonstrate that our calculation beats other existing methodologies. Regardless of the network size, the per-node communication overhead in our algorithm is o(1).

2.3) 'Securing node capture attacks for hierarchical data aggregation in wireless sensor networks'.
AUTHORS: Bhoopathy, V., Parvathi, R.M.S.:

In this study, we propose a securing hub catch assaults for progressive information total in remote sensor systems. At first system is isolated into number of bunches, every group is going by an aggregator and the aggregators are straightforwardly associated with sink. The aggregator after recognizing the distinguishing hubs chooses an arrangement of hubs arbitrarily and telecast an interesting quality which contains their validation keys, to the chose set of hubs in first round of information total. At the point when any hub inside of the gathering needs to exchange the information, it exchanges cuts of information to different hubs in that gathering, encoded by individual verification keys. Every accepting hub decodes, wholes up the cuts and exchanges the encoded information to the aggregator. The aggregator totals and encodes the information with the mutual mystery key of the sink and advances it to the sink. The arrangement of hubs is reselected with new arrangement of verification keys in the second round of total. By reenactment results, we show that the proposed strategy determines the security risk of hub catch assaults.

III. System Architecture

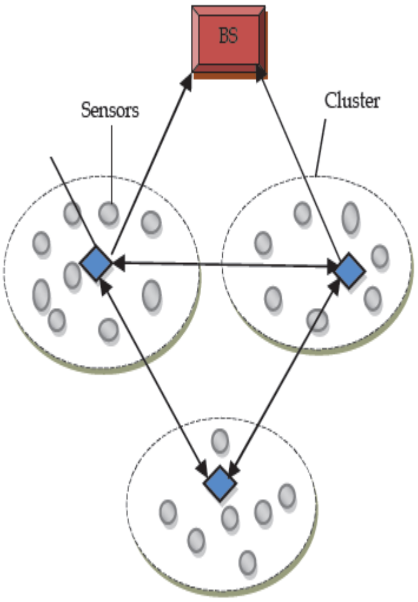

Figure 3.1 System Architecture

Fig 3.1 shows system architecture. We have proposed a genetically derived secure cluster-based data aggregation in Networks. The clustering is performed with the selection of cluster head (CH) based on the node connectivity. Within each clusters, the power consumed, distance and trust values of each member are estimated. We also propose an algorithm to choose a CH, which performs data aggregation in partially connected networks. Although the algorithm can operate in fully connected network.

Advantages:

[1] The algorithm minimizes the traffic flow within the network using the shortest selected route.
[2] The Main advantage is downloading the file at the time of forward traffic process.
[3] Minimizes the energy consumption.
[4] Ensures data security.

2.4) Modules:

2.4.1 Cluster formation.

Clustering is performed using generic algorithm. This technique highly minimizes energy consumption and thereby enhancing the network lifetime.

2.4.2 Forming data aggregation.

Initially, the CHs are chosen based on the node connectivity, which acts as a data aggregator (DAG). An improvement over the above approach would be clustering where each node sends data to cluster-head (CH) and then cluster-head perform aggregation on the received raw data and then send it to sink.

2.4.3 Data Encryption and Data Decryption.

This technique provides the secure communication framework that verifies the DP and drops the false DPs from malicious nodes.

IV. Conclusion

In this paper, we have proposed a GDSDA in Networks. At first the CHs are picked taking into account the node connectivity, which acts as a DAG. At that point, the clustering procedure is executed using the genetic algorithm. This system profoundly minimizes energy utilization and in this way improving the system lifetime. At the point when the cluster member needs to transmit information to the aggregator, an information encryption procedure are used. The CyM used offers privacy to the DP, hence guaranteeing the realness and honesty of the detected information.

References

[1]. Makin, B.A., Padha, D.A.: 'A trust-based secure data aggregation protocol for wireless sensor networks', IUP J. Inf. Technol., 2010, VI, (3), pp. 7

[2]. Roy, S., Conti, M., Setia, S., Jajodia, S.: 'Secure data aggregation in wireless sensor networks', IEEE Trans. Inf. Forensics Sec., 2012, 7, (3).

[3]. Jha, M.K., Sharma, T.P.: 'A new approach to secure data aggregation protocol for wireless sensor network', Int. J. Comput. Sci. Eng. (IJCSE), 2010, 02, (05), pp. 1539–1543

[4]. Patil, N.S., Patil, P.R.: 'Data aggregation in wireless sensor network'. IEEE Int. Conf. Computational Intelligence and Computing Research, 2010

[5]. Bhoopathy, V., Parvathi, R.M.S.: 'Securing node capture attacks for hierarchical data aggregation in wireless sensor networks', Int. J. Eng. Res. Appl., 2012, 2, (2), pp. 466–474

[6]. Jha, M.K., Sharma, T.P.: 'A new approach to secure data aggregation protocol for wireless sensor network', Int. J. Comput. Sci. Eng. (IJCSE), 2010, 02, (05), pp. 1539–1543

[7]. Sen, J.: 'A survey on wireless sensor network security', Int. J. Commun. Netw. Inf. Secur. (IJCNIS), 2009, 1, (2), pp. 55–78.

[8]. Ozdemir, S., Xiao, Y.: 'Secure data aggregation in wireless sensor networks: A comprehensive overview', Comput. Netw., 2009, 53, (12), pp. 2022–2037

[9]. Alzaid, H., Foo, E., Nieto, J.G.: 'Secure data aggregation in wireless sensor network: a survey'. Proc. Sixth Australasian Information Security Conf. (AISC), Australian Computer Society, 2008, pp. 93–105

[10]. vha, M.K., Sharma, T.P.: 'Secure data aggregation in wireless sensor network: a survey', Int. J. Eng. Sci. Technol. (IJEST), 2011, 3, (3), pp. 2013–2019

[11]. Kwon, T., Hong, J.: 'Secure and efficient broadcast authentication in wireless sensor networks', IEEE Trans. Comput., 2010, 59, (8), pp. 1120–1133

[12]. HevinRajesh, D., Paramasivan, B.: 'Fuzzy based secure data aggregation technique in wireless sensor networks', J. Comput. Sci., 2012, 8, (6), pp. 899–907

[13]. Mozumdar, M.M.R., Nan, G., Gregoretti, F., Lavagno, L., Vanzago, L.: 'An efficient data aggregation algorithm for cluster-based sensor network', J. Netw., 2009, 4, (7), pp. 598–606.

[14]. Perez-Toro, C.R., Panta, R.K., Bagchi, S.: 'RDAS: reputation-based resilient data aggregation in sensor network'. IEEE SECON 2010 Proc.

[15]. Fulare, P.S., Chavhan, N.: 'False data detection in wireless sensor network with secure communication', Int. J. Smart Sens. Ad Hoc Netw. (IJSSAN), 2011, 1, (1), pp. 66–71

[16]. Mehrjoo, S., Aghaee, H., Karimi, H.: 'A novel hybrid GA–ABC based energy efficient clustering in wireless sensor network', Can. J. Multimedia Wirel. Netw., 2011, 2, (2), pp. 41–45

[17]. Sen, J.: 'Secure and energy-efficient data aggregation in wireless sensor networks'. Proc. Second National Conf. Computational Intelligence and Signal Processing (CISP 2012), 2012

[18]. He, W., Liu, X., Nguyen, H., Nahrstedt, K., Abdelzaher, T.: 'PDA: privacy-preserving data aggregation in wireless sensor networks'. IEEE ICWMC, 2010

[19]. Yue, J., Zhang, W., Xiao, W., Tang, D., Tang, J.: 'A novel unequal cluster-based data aggregation protocol for wireless sensor networks', Prz. Elecktrotech., 2013, ISSN 0033-2097, R.89 NR 1b/2013, pp. 20–24,

[20]. Bekara, C., Laurent-Maknavicius, M., Bekara, K.: 'SAPC: a secure aggregation protocol for cluster-based wireless sensor networks', Mob. Ad Hoc Sens. Netw. Lect. Notes Comput. Sci., 2007, 4864, pp. 784–798.

[21]. Kumar, D., Aseri, T.C., Patel, R.B.: 'EECDA: energy efficient clustering and data aggregation protocol for heterogeneous wireless sensor networks', Int. J. Comput. Commun. Control, 2011, VI, (1), pp. 113–124

ABOUT AUTHOR

Sheetal Chate received B.E degree in Information Technology and Engineering from Pune University, India in 2013 and pursuing ME degree in Computer Science and Engineering from Rajarshi Shahu College of Engineering, and Pune, India.