Research Paper

Volume : 3 | Issue : 4 | Special Apr Issue 2014 • ISSN No 2277 - 8179

A Framework for Cluster Based Secure Data Aggregation Protocol for Wireless Sensor Networks

Technology & Innovation

KEYWORDS : Cluster based secure data aggregation, Cluster based approach, Wireless sensor networks, security

F.NIRMALA SHERINE Assistant Professor, Dept. Information Technology, Periyar Maniammai University, Vallam,Thanjavur, India.

V.HAMSADHWANI Assistant Professor(SS), Dept. Information Technology, Periyar Maniammai University, Vallam,Thanjavur, India.

ABSTRACT

In many sensor applications, the data collected from individual nodes is aggregated at a Cluster Heads(CHs). Wireless sensor networks often consists of sensor nodes with sensing and communication capabilities. To reduce energy consumption, many systems also perform in-network aggregation of sensor data at intermediate nodes enroute to the cluster head. Data aggregation is the process of summarizing and combining sensor data in order to reduce the amount of data transmission in the network. We focus on secure data aggregation problems for cluster based approach in WSN. The main goal of cluster based secure data aggregation in resilient aggregation protocols for both flats networks and hierarchical networks. In this paper, system designer to choose the particular network architecture depending on the capacity, energy constraints and security based on application.

INTRODUCTION

Sensor networks are increasingly deployed for applications such as wildlife habitat monitoring, forest fire prevention, and military surveillance [19,21,25]. In these applications, the data collected by sensor nodes from their physical environment needs to be assembled at a host computer or data sink for further analysis. Typically, an aggregate (or summarized) value is computed at the data sink by applying the corresponding aggregate function, e.g., MAX, COUNT, AVERAGE or MEDIAN to the collected data.

There are several factors which determine the energy efficiency of a sensor network such as network architecture, the data aggregation mechanism and the underlying routing protocol. In this paper, we describe the influence of these factors on the energy efficiency of the network in the context of data aggregation. We now present a formal definition of energy efficiency.

Energy Efficiency: The functionality of the sensor network should be extended as long as possible. In an ideal data aggregation scheme, each sensor should have expended the same amount of energy in each data gathering round. A data aggregation scheme is energy efficient if it maximizes the functionality of the network. If we assume that all sensors are

equally important, we should minimize the energy consumption of each sensor. This idea is captured by the network lifetime which quantifies the energy efficiency of the network.

Network lifetime, data accuracy, and latency are some of the important performance measures of data aggregation algorithms. The definitions of these measures are highly dependent on the desired application. We now present a formal definition of these measures.

Network lifetime: Network lifetime is defined as the number of data aggregation rounds till a% of sensors die where a is specified by the system designer. For instance, in applications where the time that all nodes operate together is vital, lifetime is defined as the number of rounds until the first sensor is drained of its energy.

Data accuracy: The definition of data accuracy depends on the specific application for which the sensor network is designed. For instance, in a target localization problem, the estimate of target location at the sink determines the data accuracy.

Latency: Latency is defined as the delay involved in data transmission, routing and data aggregation. It can be measured as the time delay between the data packets received at the sink and the data generated at the source nodes. In this survey paper, we present an extensive overview of several data aggregation algorithms. We first present the basic functionality of the specific algorithm being described and its distinct features. We then discuss the performance of the algorithm and compare it with other similar approaches.

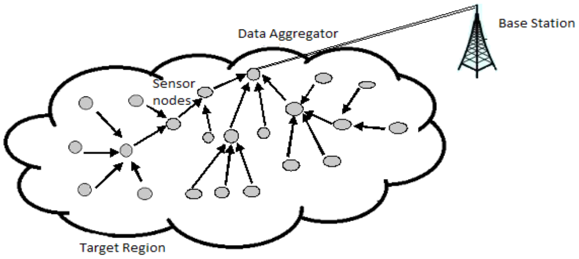

Fig.1. Data aggregation in wireless sensor network

1. RELATED WORK

Security requirements of wireless sensor networks Due to hostile environments and unique properties of wireless sensor networks, it is a challenging task to protect sensitive information transmitted by wireless sensor networks [1]. Fig. 2 illustrates the interaction between wireless sensor network security requirements and data aggregation process.

1.1 Data Confidentiality

In wireless sensor networks, data confidentiality ensures that secrecy of sensed data is never disclosed to unauthorized parties and it is the most important issue in mission critical applications. Authors of [4] state that a sensor node should not leak its readings to neighboring nodes.

2.2 Data integrity and Freshness

Data aggregation results in alterations of data; therefore, it is not possible to have end-to-end integrity check when data aggregation is employed. Moreover, if a data aggregator is compromised, then it may corrupt sensor data during data aggregation and the base station has no way of checking the integrity of this aggregated sensor data..

2.3. Source authentication

The sender and the receiver share a secret key to compute the message authentication code (MAC) for all transmitted data. However, data aggregators may need broadcast authentication which requires more complex techniques, such as lTESLA [5].

2.4. Availability

Availability guarantees the survivability of network services against Denial-of-Service (DoS) attacks. A DoS attack can be launched at any layer of a wireless sensor network and may disable the victim node(s) permanently. In addition to DoS attacks, excessive communication or computation may exhaust battery charge of a sensor node. Consequences of availability loss may be catastrophic.

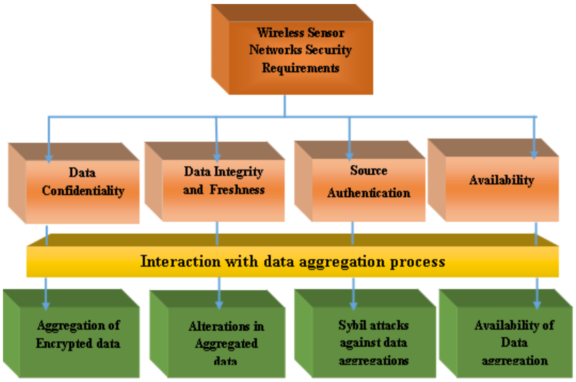
Wireless Sensor Networks Security Requirements
Data Confidentiality
Data Integrity and Freshness
Source Authentication
Availability
Interaction with data aggregation process
Aggregation of Encrypted data
Alterations in Aggregated data
Sybil attacks against data aggregations
Availability of Data aggregation

Fig. 2. Interaction between wireless sensor network security and data aggregation process.

important than regular sensor nodes. Thus, in wireless sensor networks, intruders launch DoS attacks with the aim of preventing data aggregators from performing their task so that some part of the network losses its availability.

Some Secure Aggregation Schemes

- Secure Aggregation for Wireless Networks (SAWN)
- A Secure Data Aggregation and Verification Protocol for Sensor Networks (SecureDAV)
- A Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks (SDAP)
- Secure Hierarchical In-Network Aggregation in Sensor Networks (SHDA)

3. PROPOSED SYSTEM

Framework of Cluster Based Secure Data Aggregation

In cluster-based data aggregation protocols, sensor nodes are subdivided into clusters. In each cluster, a cluster head is elected in order to aggregate data locally and transmit the aggregation result to the base station. Cluster heads can communicate with the sink directly via long range radio transmission.

LEACH is a clustered approach where cluster heads act as data aggregation points. The protocol consists of two phases. In the firstphase, cluster structures are formed. Then, in the second phase, cluster heads aggregate and transmit the data to the base station. LEACH's cluster head election process is based on a distributed probabilistic approach as follows. In each data aggregator selection round, sensor nodes calculate the threshold $T(n)$:

$$T(n) = \begin{cases} \frac{P}{1-P(R mod(1/P))} & \text{if } n \in G, \\ 0 & \text{otherwise.} \end{cases}$$

Here P is the desired percentage of cluster heads, R is the round number, and G is the set of nodes that have not been cluster heads during the last 1=P rounds. In order to be a cluster head, a sensor node n picks a random number between [0,1] and becomes a cluster head if this number is lower than TðnÞ..

HEED defines the average of the minimum power level required by all sensor nodes within the cluster to reach the cluster head. This is called Average Minimum Reachability Power (AMRP). AMPR is used to estimate the communication cost in each cluster. In order to select cluster heads, each sensor node computes its probability of becoming the cluster head as follows:

$$P_{(CH)} = C \times \frac{E_{residual}}{E_{max}},$$

where C and Eresidual and Emax denote the initial percentage of cluster heads, the current residual, and initial energy of the sensor node, respectively.As in LEACH, cluster heads in HEED, communicate directly with the base station.

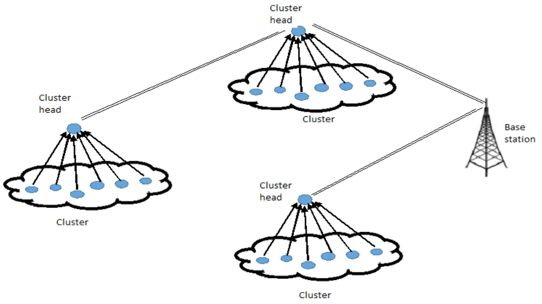

Fig.3. Cluster – based data aggregation

Once cluster heads aggregate their cluster data, they send the local aggregated data to a gateway node. Similar to LEACH, Cougar is negatively affected by dynamic network topologies.

Secure data aggregation

However, the resource constrained sensor nodes and necessity of plain data for aggregation process pose great challenges when implementing security and data aggregation together. Security requirements of wireless sensor networks can be satisfied using either symmetric key or asymmetric key cryptography.

That is, data aggregators must decrypt every message they receive, aggregate the messages according to the corresponding aggregation function, and encrypt the aggregation result before forwarding it. In addition, these schemes require data aggregators to establish secret keys with their neighboring nodes.

Secure data aggregation using plain sensor data

Earlier work on secure data aggregation is focused on symmetric key cryptography and aggregation of plain data. In [26], the authors propose security mechanisms to detect node misbehavior (dropping, modifying or forging messages, transmitting false aggregate value).

4. RESULTS AND DISCUSSION

Any secure data aggregation protocol can be roughly divided into three main phases.

Bootstrapping phase

- The bootstrapping phase in any system is one where the infrastructure is initialized to carry out the intended task.
- With respect to wireless sensor networks, bootstrapping deals with setting up the network and the keys to carry out secure communication

Data aggregation phase

- The encryption and decryption operations are computationally expensive and time consuming, end to end encryption helps save resources.
- To achieve end to end security, we need a way to aggregate data without having to decrypt it during the time it is in the network .

Integrity verification phase

- At the end of the data aggregation phase, the base station receives encrypted data from the network.
- Encryption of data ensures that any unauthorized party, which does not have the encryption key, is not able to see the data.
- How do we counter a malicious node inside the network which may be injecting false data?
- The purpose of this phase is to make sure that any tampering of the original data is detected.
- Digital signatures are the most common method to keep a check on the integrity of data.

Clustered Aggregation (CAG), mechanism was proposed, which utilizes the spatial correlation of sensory data to further reduce the number of transmissions by providing approximate results to aggregate queries. CAG guarantees the result to be within a user-specified error-tolerance threshold. It's performed while queries are disseminated to the network (query phase), where clusters group nodes sensing similar values. Subsequently, CAG enters the response phase wherein only one aggregated value per cluster is transmitted up the aggregation tree.

5. CONCLUSION

Generally, clustering in WSNs has been of high interest in the last decade and there is already a large number of related published works. HC structures facilitate the efficient data gathering and aggregation independent to the growth of the WSN, and generally reduce the total amount of communications as well as the energy spent. The main objective of most of the existing protocols lies on how to prolong the life time of the network and how to make a more efficient use of the critical resources. However, keeping the total overhead low, the efficient support of nodes and CHs mobility as well as the support of mobile sinks, the incorporation of several security aspects (i.e., enhanced protection needed in hostile environments when cluster-based protocols are used), the further development of efficient recovery protocols in case of CHs failure, etc.

This paper provides a detailed review of secure data aggregation in cluster based concept in wireless sensor networks. System designer to choose the particular network architecture depending on the capacity, energy constraints and security based on application. To give the motivation behind secure data aggregation, first, the security requirements of cluster based wireless sensor networks are presented and the relationships between data aggregation concept and these security requirements are explained.

REFERENCE

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, A | survey on sensor networks, IEEE Commun. Mag. 40 (8) | (2002) 102–114. | [2] J. Yick, B. Mukherjee, D. Ghosal, Wireless sensor network | survey,Comput. Networks 52 (12) (2008) 2292–2330. | [3] K. Akkaya, M. Demirbas, R.S. Aygun, The Impact of Data | Aggregation on the Performance of Wireless Sensor | Networks, Wiley Wireless Commun. Mobile Comput. | (WCMC) J. 8 (2008) 171–193. | [4] J. Newsome, E. Shi, D. Song, A. Perrig, The Sybil attack in | sensor networks: analysis and defenses, in: Proceedings of | the Third IEEE/ ACM Information Processing in Sensor | Networks (IPSN'04), 2004, pp. 259–268. | [5] A. Perrig, R. Szewczyk, D. Tygar, V. Wen, D. Culler, | SPINS: security protocols for sensor networks, Wireless | Networks J.(WINE) 2 (5) (2002) 521–534. | [6] Crossbow Technologies Inc. <http://www.xbow.com>. | [7] E. Fasolo, M. Rossi, J. Widmer, M. Zorzi, In-network | aggregation techniques for wireless sensor networks: a | survey, IEEE Wireless Commun. 14 (2) (2007) 70–87. | [8] R. Rajagopalan, P.K. Varshney, Data aggregation techniques | in sensor networks: a survey, IEEE Commun. Surveys | Tutorials 8 (4) (2006). | [9] C. Intanagonwiwat, D. Estrin, R. Govindan, J. Heidemann, | Impact of network density on data aggregation in wireless | sensor networks, in: Proceedings of the 22nd International | Conference on Distributed Computing Systems, 2002, pp. | 457–458. | [10] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, | F. Silva, Directed diffusion for wireless sensor networking, | in: IEEE/ACM Transactions on Networking, vol. 11, 2003, | pp.2–16. | [11] B. Krishnamachari, D. Estrin, S. Wicker, The impact of | data aggregation in wireless sensor networks, in: | Proceedings of the 22nd International Conference on | Distributed Computing Systems Workshops, 2002, pp. | 575–578. S. Ozdemir, Y. Xiao / Computer Networks 53 | (2009) 2022–2037 2035 | [12] M. Ding, X. Cheng, G. Xue, Aggregation tree construction | in sensor networks, in: Proceedings of the 58th IEEE | Vehicular Technology Conference, vol. 4, 2003, pp. 2168– | 2172. | [13] R. Cristescu, B. Beferull-Lozano, M. Vetterli, On network | correlated data gathering, in: Proceedings of the 23rd | Annual Joint Conference of the IEEE Computer and | Communications Societies, vol. 4, 2004, pp. 2571–2582. | [14] S. Madden et al., TAG: A Tiny Aggregation Service for | Adhoc Sensor Networks, OSDI, Boston, MA, 2002. | [15] B. Zhou et al., A Hierarchical Scheme for Data Aggregation | in Sensor Network, IEEE ICON 04, Singapore, 2004. | [16] M. Lee, V.W.S. Wong, An Energy-Aware Spanning Tree | Algorithm for Data Aggregation in Wireless Sensor | Networks, IEEE PacRrim, Victoria, BC, Canada, 2005. | [17] S. Lindsey, C. Raghavendra, K.M. Sivalingam, Data | gathering algorithms in sensor networks using energy | metrics, IEEE Trans. Parallel Distrib. Sys. 13 (9) (2002) | 924–935. | [18] G. Di Bacco, T. Melodia, F. Cuomo, A MAC Protocol for | Delay- Bounded Applications in Wireless Sensor | Networks,Med-Hoc-Net, Bodrum, Turkey, 2004. | [19] W.B. Heinzelman, A.P. Chandrakasan, H. Balakrishnan, | An application-specific protocol architecture for wireless | microsensor networks, IEEE Trans. Wireless Commun.1 | (4) (2002) 660–670. | [20] O. Younis, S. Fahmy, HEED: a hybrid, energy-efficient | distributed clustering approach for ad hoc sensor networks, | IEEE Trans. Mobile Comput. 3 (4) (2004) 366–379. | [21] Y. Yao, J. Gehrke, The Cougar approach to in-network | query processing in sensor networks, ACM SIGMOD Rec. | 31 (3) (2002) 9– 18. | [22] S. Chatterjea, P. Havinga, A dynamic data aggregation | scheme for wireless sensor networks, in: Proceedings of | the Program for Research on Integrated Systems and | Circuits, Veldhoven, The Netherlands, 2003. | [23] V. Mhatre, C. Rosenberg, Design guidelines for wireless | sensor networks: communication clustering and | aggregation, Elsevier Ad Hoc Networks J. 2(1)(2004)45– | 63. |