ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact

Mrs.Saba Sultana
Assistant Professor,
Lords Institute Of Engineering and Technology.

Mr.Kanike Srinivasulu
Lords Institute Of Engineering and Technology.

Abstract:

Serious security threat is originated by node capture attacks in hierarchical data aggregation where a hacker achieves full control over a sensor node through direct physical access in wireless sensor networks. It makes a high risk of data confidentiality. In this study, we propose a securing node capture attacks for hierarchical data aggregation in wireless sensor networks. Initially network is separated into number of clusters, each cluster is headed by an aggregator and the aggregators are directly connected to sink. 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 in first round of data aggregation. When any node within the group needs to transfer the data, it transfers slices of data to other nodes in that group, encrypted by individual authentication keys. Each receiving node decrypts, sums up the slices and transfers 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. The set of nodes is reselected with new set of authentication keys in the second round of aggregation.

INTRODUCTION:

Wireless Sensor Networks:- Wireless sensor networks consist of the latest technology that has attained notable consideration from the research community. 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.. Wireless sensor network consists of a huge number of tiny electromechanical sensor devices that are capable of sensing, computing and communicating. These electromechanical sensor devices can be made use for gathering sensory information, like measurement of temperature from an extensive geographical area . Many features of the wireless sensor networks have given rise to challenging problems . The most important three characteristics are:

- Sensor nodes 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.

Data Aggregation :-Data aggregation is considered as one of the basic dispersed data processing measures to save the energy and minimize the medium access layer contention in wireless sensor networks. It is used as an important pattern for directing in the wireless sensor networks. The fundamental idea is to 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. In addition, these operations utilize raw materials to obtain application specific information. To conserve the energy in the system thereby maintaining longer lifetime in the network, it is important for the network to preserve high incidence of the in-network data aggregation.

Hierarchical Secure Data Aggregation :-The following are the issues that are related to the security in the data aggregation of WSN :

- 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.

Generally, in wireless sensor networks for secure data aggregation, two methods can be used. They are hop by hop encrypted data aggregation and end to end encrypted data aggregation .

- Hop-by-Hop encrypted data aggregation: In this technique, the encryption of the data is done by the sensing nodes and decryption by the aggregator nodes. The aggregator nodes aggregate the data and again encrypt the aggregation result. At the end, the sink node that obtains the last encrypted aggregation result decrypts it.

- End to End encrypted data aggregation: In this technique, the aggregator nodes in between does not contain any decryption keys and can only perform aggregation on the encrypted data.

Node Capture Attacks:- 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. The blend of passive, active and physical attacks by an intellectual adversary results in node capture attack. The adversary initializes an attack by gathering the data's about WSN by overhearing something on message exchanges. This is performed either locally to single adversarial device or via entire network with the help of several adversarial devices organized in the entire network. Along with passive learning, the adversary dynamically takes part in network protocols, inquiring the network regarding the information and injecting malicious information in the network.The adversary performs the physical attacks, following active and passive learning. To enhance the function of the attack related to certain attack objective, the gathered information can be utilized to aid the adversary in choosing the sensor node.

PROBLEM STATEMENT:

Communication losses resulting from node and transmission failures, which are common in WSNs, can adversely affect tree-based aggregation approaches. To address this problem, we can make use of multi-path routing techniques for forwarding sub-aggregates. For duplicate insensitive aggregates such as Min and Max, this approach provides a fault-tolerant solution. Unfortunately, for duplicate sensitive aggregates, such as Count and Sum, multi-path routing leads to double-counting of sensor readings.

Recently, several researchers have presented clever algorithms to solve this double-counting problem. A robust and scalable aggregation framework called synopsis diffusion has been proposed for computing duplicate-sensitive aggregates. This approach uses a ring topology where a node may have multiple parents in the aggregation hierarchy. Furthermore, each sensed value or sub-aggregate is represented by a duplicate-insensitive bitmap called synopsis.

The possibility of node compromise introduces more challenges because most of the existing in-network aggregation algorithms have no provisions for security. A compromised node might attempt to thwart the aggregation process by launching several attacks, such as eavesdropping, jamming, message dropping, message fabrication, and so on. This paper focuses on a subclass of these attacks in which the adversary aims to cause the BS to derive an incorrect aggregate.

By relaying a false sub-aggregate to the parent node, a compromised node may contribute a large amount of error to the aggregate. As an example, during the Sum computation algorithm a compromised node X can inject an arbitrary amount of error in the final estimate of Sum by falsifying X's own sub-aggregate.

DRAW BACKS:

» Existing method of multi-path routing techniques for forwarding sub-aggregates. For duplicate insensitive aggregates such as Min and Max, this approach provides a fault-tolerant solution.
» Unfortunately, for duplicate sensitive aggregates, such as Count and Sum, multi-path routing leads to double-counting of sensor readings.
» Existing in-network aggregation algorithms have no provisions for security attempt to thwart the aggregation process by launching several attacks, such as eavesdropping, jamming, message dropping, message fabrication, and so on.

PROBLEM DEFINITION:

We design an algorithm to securely compute aggregates, such as Count and Sum despite the falsified sub aggregate attack. In particular, our algorithm which we call the attack-resilient computation algorithm consists of two phases.

The main idea is as follows:

(i) In the first phase, the BS derives a preliminary estimate of the aggregate based on minimal authentication information received from the nodes.

(ii) In the second phase, the BS demands more authentication information from only a subset of nodes while this subset is determined by the estimate of the first phase. At the end of the second phase, the BS can (locally) filter out the false contributions of the compromised nodes from the aggregate.

The key observation which we exploit to minimize the communication overhead is that to verify the correctness of the final synopsis (representing the aggregate of the whole network) the BS does not need to receive authentication messages from all of the nodes.

Several secure aggregation algorithms have been proposed assuming that the BS is the only aggregator node in the network. These works did not consider in-network aggregation. Recently, the research community has been paying attention to the security issues of hierarchical aggregation. Algorithm was designed in by which the BS can detect if the final aggregate, Count or Sum, is falsified. A few verification algorithms for computing aggregates within the synopsis diffusion approach were designed in recently, a few novel protocols have been proposed for secure outsourced aggregation designed for WSNs.

ADVANTAGES:

We discuss other potential problems and identify the scope of this paper falsifying the local value a compromised node C can falsify its own sensor reading with the goal of influencing the aggregate value. Falsifying the sub-aggregate a compromised node C can falsify the sub-aggregate which C is supposed to compute based on the messages received from C's child nodes. It is challenging to guard against this attack, and addressing this challenge is the main focus of this paper.

IMPLEMENTATION:
NETWORK SECURITY:

Network-accessible resources may be deployed in a network as surveillance and early-warning tools, as the detection of attackers are not normally accessed for legitimate purposes. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques. Such analysis may be used to further tighten security of the actual network being protected by the data's.

Data forwarding can also direct an attacker's attention away from legitimate servers. A user encourages attackers to spend their time and energy on the decoy server while distracting their attention from the data on the real server. Similar to a server, a user is a network set up with intentional vulnerabilities. Its purpose is also to invite attacks so that the attacker's methods can be studied and that information can be used to increase network security.

DATA AGGREGATION:

The Tiny Aggregation Service (TAG) to compute aggregates, such as Count and Average, using tree-based aggregation algorithms were proposed in algorithms to compute aggregates were proposed in treebased aggregation algorithms to compute an order-statistic (i.e., quantile) have been proposed in to address the communication loss problem in tree-based algorithms an aggregation framework called synopsis diffusion is designed in computes Count and Sum using a ring topology. Very similar algorithms are independently proposed these works use duplicate-insensitive algorithms for computing aggregates based on algorithm for counting distinct elements in a multi-set.

SECURE AGGREGATION TECHNIQUES:

Several secure aggregation algorithms have been proposed assuming that the BS is the only aggregator node in the network. These works did not consider in-network aggregation. Only recently, the research community has been paying attention to the security issues of hierarchical aggregation. The first attack-resilient hierarchical data aggregation protocol was designed in this scheme is secure when only one malicious nodes is present. A tree-based verification algorithm was designed in by which the BS can detect if the final aggregate, Count or Sum, is falsified. A few verification algorithms for computing aggregates within the synopsis diffusion approach in recently, a few novel protocols have been proposed for 'secure outsourced aggregation; however, as noted by the authors, these algorithms are not designed for WSNs.

DIFFUSION METHOD:

We further stress that our own prior work presents only a verification algorithm for the synopsis diffusion framework, which would fail in the presence of an attack. The attestation phase of SDAP can be expensively used to compute Count and Sum in the presence of a few compromised nodes. We proposed a DoS-resilient aggregation algorithm for computing Count and Sum, which is based on a novel tree sampling technique. Despite the adversarial interference, this algorithm can produce a (_, δ)–approximation of the target aggregate.Recently, the same research group has published one secure aggregation protocol that is able to pinpoint and revoke malicious nodes, even under DoS attacks. We previously presented an attack-resilient aggregation algorithm for the synopsis diffusion framework, but the current attack-resilient algorithm proposed in this paper is more efficient. We compare our current work with all the prior attack-resilient algorithms.

ATTACK RESILIENT:

Our algorithm which we call the attack-resilient computation algorithm consists of two phases. The main idea is as follows: (i) In the first phase, the BS derives a preliminary estimate of the aggregate based on minimal authentication information received from the nodes. (ii) In the second phase, the BS demands more authentication information from only a subset of nodes while this subset is determined by the estimate of the first phase. At the end of the second phase, the BS can (locally) filter out the false contributions of the compromised nodes from the aggregate. The key observation which we exploit to minimize the communication overhead is that to verify the correctness of the final synopsis (representing the aggregate of the whole network) the BS does not need to receive authentication messages from all of the nodes.

CONCLUSION:

In this paper, we have proposed Securing Node Capture Attacks for Hierarchical Data Aggregation in Wireless Sensor Networks. 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.

REFERENCES:

[1] M. Liu, N. Patwari, and A. Terzis, "Scanning the issue," Proc. IEEE, vol. 98, no. 11, pp. 1804–1807, Apr. 2010.

[2] T. Ko, J. Hyman, E. Graham, M. Hansen, S. Soatto, and D. Estrin, "Embedded imagers: Detecting, localizing, and recognizing objects and events in natural habitats," Proc. IEEE, vol. 98, no. 11, pp. 1934–1946, Nov. 2010.

[3] P. Corke, T. Wark, R. Jurdak, W. Hu, P. Valencia, and D. Moore, "Environmental wireless sensor networks," Proc. IEEE, vol. 98, no. 11, pp. 1903–1917, Nov. 2010.

[4] (2006). James Reserve Microclimate and Video Remote Sensing [Online]. Available: http://research.cens.ucla.edu/projects/2006/terrestrial/microclimate/defau%lt.htm.

[5] S. Madden, M. J. Franklin, J. Hellerstein, and W. Hong, "TAG: A tiny aggregation service for ad hoc sensor networks," in Proc. 5th USENIX Symp. Operating Syst. Des. Implement., 2002, pp. 1–3.

[6] J. Zhao, R. Govindan, and D. Estrin, "Computing aggregates for monitoring sensor networks," in Proc. 2nd Int. Workshop Sensor Netw. Protocols Appl., 2003, pp. 139–158..

[7] J. Considine, F. Li, G. Kollios, and J. Byers, "Approximate aggregation techniques for sensor databases," in Proc. IEEE 20th Int. Conf. Data Eng. (ICDE), 2004, pp. 449–460.

[8] S. Nath, P. B. Gibbons, S. Seshan, and Z. Anderson, "Synopsis diffusion for robust aggregation in sensor networks," in Proc. 2nd Int. Conf. Embedded Netw. Sensor Syst. (SenSys), 2004, pp. 250–262.

[9] M. Garofalakis, J. M. Hellerstein, and P. Maniatis, "Proof sketches: Verifiable in-network aggregation," in Proc. 23rd Int. Conf. Data Eng. (ICDE), 2007, pp. 996–1005.

[10] Y. Yang, X. Wang, S. Zhu, and G. Cao, "SDAP: A secure hop-byhop data aggregation protocol for sensor networks," in Proc. ACM MOBIHOC, 2006, pp. 356–367.

[11] H. Yu, "Secure and highly-available aggregation queries in large-scale sensor networks via set sampling," in Proc. Int. Conf. Inf. Process. Sensor Netw., 2009, pp. 1–12.

[12] S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure data aggregation in wireless sensor networks," IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp. 1040–1052, Jun. 2012.

[13] S. Roy, S. Setia, and S. Jajodia, "Attack-resilient hierarchical data aggregation in sensor networks," in Proc. ACM Workshop Security Sensor Adhoc Netw. (SASN), 2006, pp. 71–82.

[14] M. B. Greenwald and S. Khanna, "Power-conservative computation of order-statistics over sensor networks," in Proc. 23th SIGMOD Principles Database Syst. (PODS), 2004, pp. 1–11.

[15] P. Flajolet and G. N. Martin, "Probabilistic counting algorithms for data base applications," J. Comput. Syst. Sci., vol. 31, no. 2, pp. 182–209, 1985.

[16] L. Hu and D. Evans, "Secure aggregation for wireless networks," in Proc. Workshop Security Assurance Ad Hoc Netw., 2003, pp. 384–391. [17] H. Chan, A. Perrig, and D. Song, "Secure hierarchical in-network aggregation in sensor networks," in Proc. ACM Conf. Comput. Commun. Security (CCS), 2006, pp. 278–287.

[18] B. Chen and H. Yu, "Secure aggregation with malicious node revocation in sensor networks," in Proc. 31st Int. Conf. Distrib. Comput. Syst. (ICDCS), 2011, pp. 581–592.

[19] D. Wagner, "Resilient aggregation in sensor networks," in Proc. ACM Workshop Security Sensor Adhoc Netw. (SASN), 2004, pp. 68–79.

[20] L. Buttyan, P. Schaffer, and I. Vajda, "Resilient aggregation with attack detection in sensor networks," in Proc. 2nd IEEE Workshop Sensor Netw. Syst. Pervasive Comput., Mar. 2006, pp. 331–336.