Privacy Preserving Access Control On Data Aggregation For Wireless Sensor Networks

Aishwarya R and Mr. S. Sathees Babu, ASP

ABSTRACT

Wireless Sensor Network (WSN) environment is operated in vulnerable to various security attacks. Privacy is an important issue with the recent applications. Though more privacy preservation techniques are available in WSN, one of the important security measures is user access control. The related work ensures that only authorized users can access the data collected by the sensor nodes. However the single sink based data aggregation technique leads to inefficiency due to imbalance in energy consumption. In addition it induces scalability problem and overload at the sink. To overcome these issues, a modified data aggregation model with multiple sinks is proposed. In data aggregation model, the spanning tree is constructed among sensor nodes with the sink directly connected to the root sensor node and each sensor node aggregates its incoming data with its sensed value and then sends result to its present node in the tree. This can enforce the strict user access control. So that the sensed data is only accessible by the authorized users. Signature verification, key establishment and data encryption phases could possibly executed using NS2 simulator.

KEYWORDS: Access control, wireless sensor network, user privacy, accountable, Data Aggregation.

INTRODUCTION

Wireless sensor networks have very wide application prospects including both military and civilian usage. They contain supervision, tracking at critical facilities, or monitoring animal habitats. Sensor networks have the possible to drastically change the way people monitor and work together with their environment. Sensors are usually resource-limited and power-constrained. They suffer from limited computation, communication, and power resources. Sensors can supply fine-grained raw data. Alternatively, they may need to cooperate with each other on in-network processing to decrease the amount of raw data sent, thus conserving resources such as message bandwidth and energy. We refer to such in-network processing basically as data aggregation. In a lot of sensor network appliance, the fashionable is typically worried with aggregate statistics such as SUM, AVERAGE, or MAX/MIN of data readings over an assured region or period. As a result, data aggregation in WSNs has received considerable attention.

The scalability of sensor networks improves with the introduction of the multiple sinks. Efficient data gathering trees are formed by the nodes and then the best sink is chosen for transmitting the data in multiple sink networks. The mean space between the nodes and the sink will be reduced in the multi sink network leading to energy savings and improved lifetime. The sink works as a gateway in multi sink network, forwarding the sensed information near to the storage system. Only the data produced by a particular set of devices is collected by the sink. As sensor network appliances enlarge to include more and more responsive measurements of everyday life, preserving data privacy becomes an increasingly important concern.
Let us consider the example, an upcoming application might evaluate household details such as power and water usage, computing average trends and creating native recommendations. During this paper, we have a tendency to discuss a way to carry privacy-preserving data aggregation in wireless sensor networks. Future in-home floor sensors, gathering weight information, are used simultaneously with shoe-mounted sensors, collecting exercise-related information, in an obesity study to correlate exercise and weight loss. Aggregate statistics from that information are useful for organizations such as Department of Health and Human Services, as well as insurance companies for medical investigate and financial planning purposes. Though, individual’s health related information should be kept secret and not be known to other people.

From these various examples, we perceive the consequence for preserving the privacy of creature sensor readings while obtaining exact aggregate statistics can be an important requirement. The protection of privacy also gives us additional benefits including enhanced security. Consider the circumstances when an enemy compromises a part of the sensor nodes: when there is no privacy protection, the comprised nodes will hear the data messages and decrypt them to get sensitive data. However, with privacy protection, even if data are overheard and decrypted, it is still hard for the adversary to recover the sensitive data.

Consequently, providing a reasonable guideline on building systems that execute private data aggregation is attractive. It is recognized that end-to-end data encryption is capable to protect personal communications between two parties (such as the data source and data sink), as long as the two parties have agreement on encryption keys. However, end-to-end encryption or link level encryption only is not an excellent applicant for private data aggregation. This is because:

1. If end-to-end communications are encrypted, the intermediate nodes might not easily achieve in-network processing to acquire aggregated results.
2. Even when data are encrypted at the link level, the other end of the communication is still able to decrypt it and obtain the private data. Hence privacy is violated.

The objective of our work is to connection the gap between collaborative data aggregation and data privacy in wireless sensor networks. The planned sensor network can attain a explicit aggregation outcome as guaranteeing that no personal information is released to others. Observe that this is a stronger result than previously proposed protocols. Our presented schemes can be built on secure communication protocols. Therefore, both security and privacy are supported by the proposed data aggregation schemes.

**Related Works:**

More number of techniques are used to provide security in WSNs. Xu Jian et al provides a survey of privacy preserving data aggregation in Wireless Sensor Networks. Data aggregation is a very important technique, which is considered to significantly decrease the communication overhead and energy expenditure of sensor node during the process of data collection in WSNs. However, privacy-preservation is additional challenging issue in data aggregation, where the aggregators need to perform some aggregation operations on sensing data it received. We classify the presented privacy-preserving data aggregation methods into different types by the core privacy-preserving techniques used in each scheme. And then compare and contrast different algorithms on the base of performance measures such as the privacy protection ability, communication consumption, power consumption, data accuracy and aggregation function, etc. Based on the comparison result, we presented an overview of the solutions; adopt which type of privacy-preserving technique, and whether the solution is actually applicable for data aggregation in WSNs.

D.He et al describes the security vulnerabilities in data discovery and dissemination when used in WSNs. Such vulnerabilities allow an adversary to update a network with undesirable values, remove dangerous variables, or initiate denial-of-service (DoS) attacks. To deal with these vulnerabilities, this paper presents the design, implementation, and evaluation of a secure, inconsequential, and DoS-resistant data discovery and dissemination protocol named SeDrip for WSNs. Our protocol takes into consideration the limited resources of sensor nodes, data loss and out of series packet delivery. Also, it can provide instantaneous authentication without packet buffering delay, and tolerate node compromise to allow efficient authentication of the disseminated data items by taking advantage of efficient Merkle tree algorithm. SeDrip is designed to work within the computation, memory and energy limits of inexpensive sensor motes. In addition to analyzing the security of SeDrip, this paper has also reported the evaluation results of SeDrip in an experimental network of resource limited sensor nodes, which show that SeDrip is efficient and feasible in practice.

Rui Zhang et al introduced a Distributed Privacy-Preserving Access Control method for sensor networks. The owner and users of a sensor network may be different, which necessitates privacy-preserving access control. The network owner need enforce strict access control so that the sensed data are only accessible to users willing to pay. Users wish to protect their respective data access patterns whose disclosure may be used against their interests. Users in DP2AC purchase tokens from the network owner whereby to query data from sensor nodes which will respond only after validating the tokens. The use of blind signatures in token generation guarantees that tokens are publicly provable until unpleasant to user individuality, so privacy-preserving access control is achieved. A central component in DP2AC is to prevent cruel users from reusing tokens, for which we
recommend a suite of distributed token reuse detection (DTRD) schemes without concerning the base station. These schemes share the necessary scheme that a sensor node checks with some other nodes (called witnesses) whether a token has been used, but they differ in how the witnesses are selected. We meticulously evaluate their performance with observe TRD capability, communication overhead, storage overhead, and attack resilience. The efficacy and efficiency of DP2AC are confirmed by detailed performance evaluations.

Shucheng Yu et al considered Distributed sensor data storage and retrieval. Distributed architecture poses a number of security challenges especially when applied in mission-critical applications such as battlefield and e-healthcare. Initially, as sensor information are stored and maintained by individual sensors and unattended sensors are easily subject to strong attacks such as physical concession, it is significantly harder to ensure data security. Second, in more mission-critical appliances, fine-grained data access control is a necessity as prohibited access to the sensitive information may cause terrible results and be prohibited by the law. Sensor nodes usually are resource-constrained, which limits the direct adoption of expensive cryptographic primitives. To deal with the above issues, we include a distributed data access control method that is able to enforce fine-grained access control over sensor data. In FDAC all sensor node is allocated with a set of attributes, and each user is assigned an access structure which designates the access capability of the user. The sensor data are encrypted under the attributes such that only the users with the intended access structure are able to decrypt. As the access structure is extremely expressive, we are able to control data access precisely, thus achieve fine-grained access control. It is able to provide security assurance resilient against strong attacks such as sensor compromise and user colluding. It is able to support attribute change of sensor nodes and seamlessly integrate existing PH schemes to realize concealed data aggregation. The anticipated design develops a cryptographic primitive algorithm called attribute-based encryption (ABE), tailors, and adapts it for WSNs with reverence to both performance and security requirements.

Daojing He et al, describes how to protect user’s identity privacy when a user is verified by the network for data accesses. The proposed system uses Pricess protocol, to ensure distributed privacy-preserving access control. In Pricess, users who have similar access privileges are organized into the same group by the network owner. A network user signs a query command on behalf of his group and then sends the signed query to the sensor nodes of his interest. The signature can be verified by its recipient as coming from someone authorized without exposing the actual signer. Our experiment shows that the system overhead of the proposed protocol is reasonable in practical scenarios.

In the existing system security is one of the major issues in WSNs and complication with data privacy and data protection in multiple sink based data aggregation. In most existing privacy-preserving data aggregation, the actual content of sensory data should be changed its appearance (by encrypt, conceal, slice or perturb) to preserve the privacy, but the data concealment feature may be injured by compromised sensors to modify or ill-process data without being caught. Hence the proposed work is to overcome the drawbacks in the existing system.

**Network Architecture:**

Figure 1 describes a WSN which comprises of numerous users, a large number of resource-constrained sensors and a sink, one or more network owners and an off-line law authority. The sensors report their deducted data to the sink and users in reply to queries. Subsequent to enlisting to at least one network owner, network users use access devices such as smart phones or Laptop PCs to get to the detected information by sending queries to the sink or the targeted nodes. The network managers bootstrap the input resources for access devices to implement the access rights of users. According to the agreement, each network owner has specific access privilege of their own information.
Modules:
In this section, the modules for the proposed system are explained below.
There are five modules present in this proposed system to securely aggregate the data.
1. Network Formation
2. Key Generation and Distribution
3. Aggregation Request Broadcast
4. In-Network Data Aggregation
5. Performance Analysis

Network Formation:
WSN consist of many users, sensor, multiple sinks, one or more network owner and off-line law authority.
After registering to one or more network owners only, users use access devices such as laptop and or smart phones. These are used to form a small network.

![Network Formation Diagram](image)

Key Generation and Distribution:
In this phase, the user authenticates a node and a sensor node also authenticates the user; mutual authentication is thus provided between the user and the node. In some application scenarios, a session key should be established between a user and the sink to protect data communication against attacks. Here partial group public keys are only distributed. Hence the data is accessed securely.

![Key Distribution Diagram](image)

RSA:
RSA is one of the first realistic public-key cryptosystems and is generally used for secure data transmission. In such a cryptosystem, the encryption key is public and be different from the decryption key which is kept secret. RSA is based on the sensible complexity of factoring the product of two huge prime numbers,
the factoring is the problem. A user of RSA creates and then distributes a public key based on two large prime numbers, along with a supporting value. The prime numbers must be kept secret.

**Elliptic Curve Diffie-Hellman:**  
Elliptic Curve Diffie–Hellman is an ambiguous key procedure convention that acknowledges two gatherings, each having an elliptic bend public–private key match, to make a common mystery over an uncertain channel. This shared secret can be directly used as a key, or to derive another key which can then be used to encrypt subsequent communications using a symmetric key cipher.

**Aggregation Request Broadcast:**  
Before accessing the sink node, first we have to aggregate the data at the sink node. Because, the sink node directly connects to the starting node and sends to the aggregation request message identified by the seed, a number unique to each round of data aggregation. Starting node is the root node of the aggregation tree. The aggregation request message is added with the keyed values. After receiving the broadcast request, including a keyed value will communicate the access request to each of its children, along with the new key.

![Fig. 4: Aggregation Request Broadcast](image)

**In-network Data Aggregation:**  
In the aggregation phase, each leaf node computes the keyed values based on the random keys assigned to it and that Parent allowed to be used. Then the leaf node will submit its randomized values into the aggregation along with the actually used keys back to its parent node. Each non-leaf node first aggregates the values received from its children, then adds to that result both its sensed value and its own keyed values. The final aggregation result will be sent to a parent node.

![Fig. 5: In-network Data Aggregation](image)

**Performance Analysis:**  
In this phase to evaluate the performance measurements based on the memory overhead, message overhead, energy consumption and execution time. It is a comparative study with the existing study. The memory overhead specifies the amount of data space consumed by the real implementation. The message overhead
When deciding which communication mode to use, how much time your process will spend waiting for the send (or receive) to return. The execution time or CPU time of a predetermined work is depicted as the time spent by the framework executing that work, including the time spent executing runtime or framework benefits for its behalf.

Table I describes the comparative study of the execution time with the proposed system. Here we compare the execution time for multiple sinks. Execution time is calculated at ms. For sink 1 the execution time for the existing system is 7.761ms. But our proposed system takes only 6.612ms. That will improve the performance of the system.

Table II describes the energy consumption for multiple sinks. If the energy consumption rate increases then the performance of the system decreases. Hence our proposed system reduces the energy consumption. For example in sink 2 the energy consumption rate of the existing system is 5.4405 and the proposed system is 4.9862.

Table III describes the message overhead Message overhead for multiple sinks. Message increases the data loss. Hence that will damage the data accuracy. To avoid this data loss we have to reduce the data loss. It will improve the system performance. For example in sink 5 the message overhead for the existing system is 412 bytes and the proposed system is 348 bytes.

![Execution Time Analysis Graph](image-url)

**Table I**: The Execution Time For Sink Nodes

<table>
<thead>
<tr>
<th>Sink</th>
<th>Execution time APAC(ms)</th>
<th>Execution time APAC with modified data aggregation(ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sink 1</td>
<td>7.761</td>
<td>6.612</td>
</tr>
<tr>
<td>Sink 2</td>
<td>8.663</td>
<td>7.543</td>
</tr>
<tr>
<td>Sink 3</td>
<td>6.945</td>
<td>5.986</td>
</tr>
<tr>
<td>Sink 4</td>
<td>5.867</td>
<td>5.432</td>
</tr>
<tr>
<td>Sink 5</td>
<td>5.396</td>
<td>4.875</td>
</tr>
<tr>
<td>Sink 6</td>
<td>4.476</td>
<td>4.312</td>
</tr>
</tbody>
</table>

**Table II**: The Energy Consumption For Sink Nodes

<table>
<thead>
<tr>
<th>Sink</th>
<th>Energy consumption APAC(mJ)</th>
<th>Energy consumption APAC with modified data aggregation(mJ)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sink 1</td>
<td>3.6888</td>
<td>3.5021</td>
</tr>
<tr>
<td>Sink 2</td>
<td>5.4405</td>
<td>4.9862</td>
</tr>
<tr>
<td>Sink 3</td>
<td>1.8812</td>
<td>1.0032</td>
</tr>
<tr>
<td>Sink 4</td>
<td>4.7985</td>
<td>3.9078</td>
</tr>
<tr>
<td>Sink 5</td>
<td>2.4351</td>
<td>1.3294</td>
</tr>
<tr>
<td>Sink 6</td>
<td>3.875</td>
<td>2.7640</td>
</tr>
</tbody>
</table>

**Table III**: The Message Overhead For Sink Nodes

<table>
<thead>
<tr>
<th>Sink</th>
<th>Message overhead APAC(bytes)</th>
<th>Message overhead APAC with modified data aggregation(bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sink 1</td>
<td>812</td>
<td>758</td>
</tr>
<tr>
<td>Sink 2</td>
<td>643</td>
<td>562</td>
</tr>
<tr>
<td>Sink 3</td>
<td>458</td>
<td>349</td>
</tr>
<tr>
<td>Sink 4</td>
<td>542</td>
<td>531</td>
</tr>
<tr>
<td>Sink 5</td>
<td>412</td>
<td>348</td>
</tr>
<tr>
<td>Sink 6</td>
<td>638</td>
<td>200</td>
</tr>
</tbody>
</table>
Figure 6 describes the analysis of the execution time for multiple sinks with its existing system. Here x-axis denotes the sink nodes and y-axis denotes the execution time in ms. In this graph, the execution time for the proposed system decreases as the performance of the system increases.

Figure 7 describes the analysis of the energy consumption for multiple sinks with its existing system. Here x-axis denotes the sink nodes and the y-axis denotes the energy rate in mJ. Y-axis takes 0-6 values for the interval 1.

Figure 8 describes the analysis of the message overhead for multiple sinks with its existing system. In this graph, the x-axis denotes the sink values, and the y-axis denotes the message overhead at bytes. It takes values from 0-900 with the interval 100. All the above graphs conclude that our proposed system provides better performance of the system.

Conclusion:
We have proposed a modified data aggregation with multiple sinks in APAC protocol, which is the primary endeavor to set up a responsible acquire to control structure with a modern client security insurance demonstrate custom-made for WSNs. The security analysis has shown APAC can accomplish the necessities of the convention of this kind.

REFERENCES