Oriental Journal of Computer Science & Technology Vol. **3**(1), 149-153 (2010)

Secure data aggregation using mobile agents in wireless sensor networks

BHAVNA ARORA MAKIN[1] and DEVANAND PADHA[2]

[1]Model Institute of Engineering & Technology, Jammu Kot Bhalwal, Jammu (India).
[2]Department of Computer Science and IT, University of Jammu, Jammu (India).

(Received: May 28, 2010; Accepted: June 21, 2010)

ABSTRACT

Data aggregation is a widely used technique in wireless sensor networks. The security issues, data confidentiality and integrity, in data aggregation become vital when the sensor network is deployed in a hostile environment. There have been many related work proposed to address these security issues. In this paper, we introduce the concept of mobile agents for secure data aggregation in sensor networks. We propose an algorithm that can be used to track a malicious node in the network and hence maintain data confidentiality and data integrity in data aggregation.

Keywords: Wireless Sensor Networks, data aggregation, mobile agents.

INTRODUCTION

Wireless sensor networks constitute an emerging technology that has received significant attention from the research community.A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants.

Sensor networks are typically self-organizing adhoc systems that consist of many small, low-cost devices.In addition to one or more sensors, each node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a small microcontroller, and an energy source, usually a battery.Typically, the radio transmission range of the sensor nodes are typically orders of magnitude smaller than the geographical extent of the entire network.

They monitor the physical environment, and subsequently gather and relay information to one or more sink nodes.The data needs to be aggregated before it is relayed towards the sink. The aggregation of data is recognized as one of the basic distributed data processing procedures in wireless sensor networks for saving energy and reducing medium access layer contention[6]. The idea is to combine the data coming from different sources enroute – eliminating redundancy, minimizing the number of transmissions and thus saving energy[7]. The aggregator uses specific functions, such as addition, subtraction or exclusive or, to aggregate incoming readings, and only aggregated result are forwarded. Thus, routing and data aggregation are strongly interconnected issue. Therefore, communication overhead can be reduced by decreasing the number of transmitted packets.

Security issues of data aggregation

Secure Data Aggregation

The security issues in the data aggregation of WSN are given below[8].

1. Data Confidentiality

Specifically, the fundamental security issue is data confidentiality which protects the sensitive transmitted data from passive attacks, such as eavesdropping. Data confidentiality is especially vital in a hostile environment, where the wireless channel is vulnerable to eavesdropping.

2. Data Integrity

It prevents the compromised source nodes or aggregator nodes from significantly altering the final aggregation value. Sensor nodes are easy to be compromised because they lack expensive tampering-resistant hardware, and even that tampering-resistant hardware might not always be reliable. A compromised node can modify, forge or discard messages.

3. Intoduction to Mobile agents

A mobile agent is a composition of software and data, which is able to migrate from one node to another autonomously in a network and continue its execution on the destination node. A mobile agent has the unique ability to transport itself from one system in a network to another in the same or heterogeneous networks. Mobile agents can be rapidly deployed, and can respond to each other and their environment.

These features of mobile agents will help us in our model to propose for secure data aggregation.

4. Background

The Network Model

We consider a similar model with[5] in which the nodes in the WSN can be divided into four sets *S;A;F* and *R*:

1) *S* is the set of sensing nodes, which sense their environment;
2) *A* is the set of aggregator nodes, which combine the sensing values from *S* by aggregation functions;
3) *F* is the set of forwarders, which transfer the aggregation results from *A* towards *R* hop-by-hop;
4) *R* is the set of readers of the WSN, which may be base stations, or merely the sinks which provide an access to the outside for the WSN.

Also *S;A;F;R* may change over time and their intersections may not be *Á*.

The network model can represent both the Hierarchical WSN (HWSN) and Distributed WSN (DWSN). In HWSN, nodes are deployed hierarchically according to their capabilities. The whole network is composed of base stations (ª *R*), cluster heads (ª *A U F*) and sensor nodes (ª *S*). In DWSN, nodes are deployed randomly in the environment. After nodes are deployed, a transmission structure should be constructed to aggregate data. For example, in [24] a minimum spanning tree (MST) is constructed to gather data with minimum energy cost in WSN. In the MST, the root node (sink) is in the reader set *R*, every node in the WSN is in *S*, every non-leaf node is in the aggregator set *A* and the forwarder set *F*. The non-leaf nodes aggregate the data they received with their own sensing data.

Vulnerabilities of attacks

We assume there is only one adversary in the WSN, it is a polynomial-time bounded probabilistic Turing machine, it can physically access the sensors and read their internal values. The adversary is also assumed to be restricted in one region, so it can only compromise a small number of sensors.

An adversary can breach the data confidentiality by the following attacks:

1) eavesdropping the messages in the wireless channel;
2) compromising a node and obtaining all keys stored in it;
3) using the compromised node's keys to deduce the keys employed elsewhere in the network;
4) using the compromised node's keys to inject unauthorized malicious sensor nodes in the network.

The adversary can also spoil the data integrity by the following attacks:

1) injecting arbitrary chosen malicious data into the compromised sensing nodes in the set *S*;
2) modifying, forging, or discarding messages in the compromised aggregator nodes in *A* and compromised forwarder nodes in *F*.

Aggregation functions

Given the sensing data *si* from the sensing node *Si* in *S* for *i* = 1*; :::; n*, the following aggregation function *f*(*s*1*; :::; sn*) can be calculated in the WSN:

1) the *Sum*: $f(s_1,..,s_n) = \sum_{i=1}^{n} si$.
2) the *Average*: $f(s_1,..,s_n) = \sum_{i=1}^{n} si/n$.
3) the *Median*:$f(s_1,..,s_n) = s(_r)$, $r = (n + 1)=2$, $s(_1)...s(_n)$ is an sorted order of $s1,. sn$. 4) the *Minimum*: $f(s_1,..,s_n) = min\{ s_1 \ li= 1,..,n\}$. 5) the *Maximum*: $f(s_1,..,s_n)= max\{ s_1 \ li= 1,..,n\}$. 6) the *Count*: $f(s_1,..,s_n)$ =count$\{ s_1 \ li= 1,..,n\}$.

5. Our Contributions

We propose a mobile agent based security algorithm to determine whether a malicious node has joined in the network. If there is a detection as such then the node is discarded from any further activity of any type. We use the concept of mobile agents because of the following features –

1. Small byte code.
2. Ability to travel in the network independently and can travel in a predefined path.

Assumption

We assume that the network model is HWSN. We consider the model as stated in the section4. The WSN contains four types of nodes(R,S,F & A) as discussed.

Let $R=\{r_1,r_2,r_3,\ldots,r_{n1}\}$ –The set of readers
$F=\{f_1,f_2,f_3,\ldots,f_{n2}\}$- The forwarders
$A=\{a_1,a_2,a_3,\ldots,a_{n3}\}$-The aggregators
$S=\{s_1,s_2,s_3,\ldots s_{n4}\}$-The Sensors

Here the problem of traversing (n1+n2+n3+n4) =N (no. of nodes of the minimum spanning tree) corresponding to WSN which may be considered as a connected weighted graph where the quantitative weightage of each pair of nodes is pre-determined in terms if distance /cost/ time etc.

Matrix representation of the minimum spanning tree of n1 no.of R,n2 no.of F , n3 no. of A and n4 no.of S

	R	F	A	S
R				
F				
A				
S				

Let (ai bj) be the element of the matrix then
(ai ai)=(bj bj)=0 and (ai bj)#0
Hence

Σ (ai bj)= Total of weight ages in each row of the matrix.

Figure 1 shows the pictorial representation of the above said structure

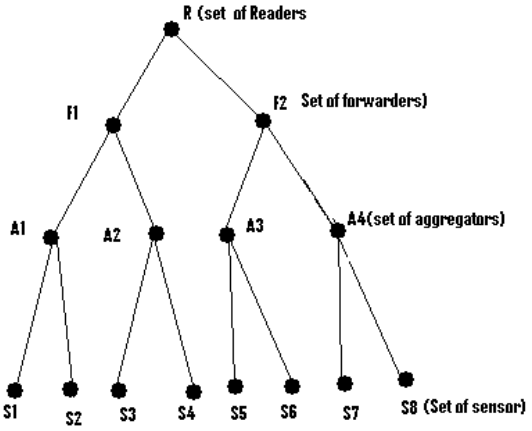

Figure 1.

In our algorithm we propose that the mobile agent will have the capability of travelling from the sensor node via the aggregator and forwarder to the reader and back. All consistent nodes are registered at the Reader/sink. Change in any configuration will be checked back with the sink and will be assumed that there is a malicious node that has joined in. In case of any such adversary the node is discarded from the network and will be disqualified from participating in any kind of activity in the network. Correspondingly the registration of that node at the sink will also be affected and the node be marked as invalid. As the nodes that exist within a WSN are large, clusters can be formed and agents can be deployed per cluster.

Alogrithm

1. Deploy new S (sensing node)
2. Register at Reader/Sink(R)
3. Refresh tree structure
4. Delete existing mobile agent(*m_old*) if any
5. Create new mobile agent *m* at R
6. Span tree and gather information of all nodes (node –id and type) and cross check at R in a predetermined procedure.
7. Agent keeps spanning tree.
8. S senses environment and collects data

9. S send data to A (aggregator nodes)
10. On_receive_data_at_A

```
Procedure_aggregation()
{
Check_validity_of_S()
{
Check_node_with_agent()
{ if valid_node()
Flag=1;
Else
Flag=0;
}
If flag=0
Check_node_with_R()
{
list=Get_list_of_valid_nodes_from_R_through_agentm
();
Linear search(list) // for valid node id
If Valid_id(S)
Flag=1;
Else
Flag=0;
}}
If flag=1
Aggregate_data(S);
If flag=0
Reject_data(S);
Report_to_reader(Malicious node S);
}
```

11. Go to 4.

Corollaries-

Case 1:Addition of new node-

```
Add_new_node(S)
{
Deploy new  S (sensing node)
Register at R
Refresh tree structure
Update Agent
}
```

Case 2:Deletion of a node

```
Delete_node(S)
{
de-register at R
Refresh tree structure
Update Agent
}
```

Discussion of Algorithm

1. Ease of implementation
2. Energy efficiency- is slightly low as each time there is an adversary the tree structure needs to be refreshed and the mobile agent needs to be deleted and then recreated.
3. Spanning of tree by mobile agents need to be very fast as there could be any attack as soon as the agent leaves a node.

6. Conclusion and Future scope

Recent years have witnessed a growing interest in deploying large numbers of micro sensors that collaborate in a distributed manner on data gathering and processing. The issues on secure routing still remain open to much extent. Lot of work is being done in this area and a lot need to be done. Recently ,Mobile agents have been proposed for efficient data dissemination in WSN. Mobile agents, due to their small byte code and their ability to travel in the network independently and a predefined path are gaining a significance attention in WSN's as well. The energy efficiency and well deployment of these agents in WSN is still a challenge.

We have proposed a approach that uses mobile agents for detecting malicious nodes. The algorithm is easy to implement but has the overhead of deploying mobile agents. The issues that still remain open are the efficiency of the agent and probability of mobile agent detecting malicious nodes in a WSN as the agent would always be on a move trying to detect any malicious node that joins the networks.

REFERENCES

1. Yingpeng Sang, Hong Shen, Yasushi Inoguchi, Yasuo Tan and Naixue Xiong, "Secure Data Aggregation in Wireless Sensor Networks: A Survey", Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies,

(2006).

2. Prakash G L, S H Manjula, K R Venugopal and L M Patnaik, "Secure Data Aggregation Using Clusters in Sensor Networks", International Journal of Wireless Networks and Communications. **1**(1), pp. 93–101 (2009).
3. Chris Karlof and David Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures", Proceedings of the First IEEE International Workshop on In Sensor Network Protocols and Applications, (2003).
4. Min Chen, Taekyoung Kwon, Yong Yuan, and Victor C.M. Leung, "Mobile Agent Based Wireless Sensor Networks", In Journal ofComputers, Vol. 1, NO. 1, pp.14-21, (2006).
5. 5 . E. Mykletun, J. Girao, and D. Westhoff, "Public key based cryptoschemes for data concealment in wireless sensor networks", in IEEE International Conference on Communications (ICC2006), (2006).
6. Zhenzhen Ye, Alhussein A. Abouzeid and Jing Ai, "Optimal Policies for Distributed Data Aggregation in Wireless Sensor Networks", Draft Infocom (2007).
7. Bhaskar Krishnamachari, Deborah Estrin and Stephen Wicker, "The Impact of Data Aggregation in Wireless Sensor Networks", Proceedings of the 22nd International Conference on Distributed Computing Systems (2002).
8. Yingpeng Sang, Hong Shen, Yasushi Inoguchi, Yasuo Tan and Naixue Xiong, "Secure Data Aggregation inWireless Sensor Networks: A Survey", Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies, 2006.
9. Kai-Wei Fan, Sha Liu, and Prasun Sinha, "Structure-free Data Aggregation in Sensor Networks", IEEE Transactions on Mobile Computing (2007).