Power Efficient Data Fusion Assurance Scheme for Sensor Network using Silent Negative Voting

M.Umashankar
K.S.Rangasamy College of Technology
Tiruchengode, Tamilnadu, INDIA

Dr.C.Chandrasekar
Periyar University
Salem, Tamilnadu, INDIA

ABSTRACT
Security is a very important issue when designing or deploying any network or protocol. The nature of large, ad-hoc, wireless sensor networks presents significant challenges in designing security schemes. One or several sensors then collect the detection results from other sensors. The collected data must be processed by the sensor to reduce the transmission burden before they are transmitted to the base station. This process is called data fusion. Data fusion Nodes will fuses the collected data from nearby sensor nodes before they are sent to the base station. If a fusion node is compromised, then the base station cannot ensure the correctness of the fusion data sent to it. Various methods are proposed, that deal with providing an assured data transfer to the Base Station.

In this paper a novel power-efficient data fusion assurance scheme has been proposed using silent negative voting mechanism. The proposed scheme has been compared with the direct voting based fusion assurance scheme. The proposed scheme produced very well with better power efficiency and lower network overhead.

Keywords: Sensor Network, Data Fusion, Fusion Assurance, Security

1. INTRODUCTION

1.1 Wireless Sensor Networks
A wireless sensor networks (WSNs) are consists of inexpensive sensor nodes, each node having continuous sensing capability with limited communication power [6]. They can be used for several applications such as Commercial, civil, and military applications including vehicle tracking, climate monitoring, intelligence, medical and agriculture, etc. Sensor nodes are having inbuilt chips and Software for processing specific function. The security application of a Wireless sensor network would give some one the ability to collect and analyze data remotely and detect any kind of attack. In the Military applications they are used wireless sensor networks to collect such sensitive data the information passed over the nature would have to be secure. However, Sensor networks are relatively more insecure repository and routers of data, which increased the need of new security schemes. Their deployment in environments disaster areas, earthquake/rubble zones or in military battlegrounds can be seriously affected by any kind of sensor failure or malicious attack/security threats from an enemy.

Sensor nodes are self powered and equipped with low computational power CPU allowing the sensor to execute some kind of treatment before sending a report to the centralized authority.

1.2 Sensor Security Challenges
Due to Hostile environments, it is a challenging task to protect sensitive information transmitted by wireless sensor networks [7]. Security is an important issue for wireless sensor networks and there are many security considerations that should be investigated[8]. When designing or deploying any network or protocol, the nature of large, ad-hoc, wireless sensor networks presents significant challenges in designing security schemes.

In this Section we present five of the most pronounced challenges:

1.2.1 Wireless Medium
The wireless medium is inherently less secure because its broadcast nature makes eavesdropping simple. Any transmission can easily be intercepted, altered, or replayed by an adversary.

1.2.2 Ad-Hoc Deployment
The network topology is always subject to changes due to node failure, addition, or mobility. Nodes may be deployed by air drop, so nothing is known of the topology prior to deployment. Since nodes may fail or be replaced the network must support self-configuration.

1.2.3 Hostile Environment
A third challenging factor is the hostile environment in which sensor nodes function. Sensor nodes face the possibility of destruction or capture by attackers. Since nodes may be in a hostile environment, attackers can easily gain physical access to the devices.

1.2.4 Resource Scarcity
The extreme resource limitations of sensor devices pose considerable challenges to resource-hungry security mechanisms. Security mechanisms must give special effort to be communication efficient in order to be energy efficient.

1.2.5 Immense Scale
Finally, the scale of sensor networks poses a significant challenge for security mechanisms. Simply networking tens to hundreds of thousands of nodes has proven to be a substantial task. Providing security over such a network is equally challenging. Security mechanisms must be scalable to very large networks while maintaining high computation and communication efficiency.

1.3. Data Fusion
In General the Wireless Sensor Networks are consists of several sensor nodes because a single sensor is not sufficient for the compensation and correction of internet and uncertain information, it is necessary to add additional sensors. Multiple sensor data fusion is an emerging technology, concerning the problem of how to fuse data from multiple sensors in order to make a more accurate estimation of the environment. Applications of data fusion cross a wide spectrum, including environment monitoring, automatic target detection and tracking, battlefield surveillance, remote sensing, global

awareness, equipment maintenance, energy management, etc. They are usually time-critical, cover a large geographical area, and require reliable delivery of accurate information for their completion. So far, client/server computing model has been most popularly used in Distributed Sensor Networks (DSNs) to handle multisensory data fusion. However, as advances in sensor technology and computer networking allow the deployment of large amount of smaller and cheaper sensors, huge volumes of data need to be processed in real-time. The big challenge now is to develop effective methods for the automatic fusion and interpretation of the information generated by large-scale sensor networks. The success of future applications is predicated on finding solutions to this data fusion challenge.

Very large sensor networks and their resource constraints face a big challenge for design and develop a perfect information processing and aggregation techniques to make effective use of the aggregate data [12]. Issue a query, it may be unnecessary to return all raw data collected from each sensor, information should be processed and aggregated within the network and only processed and aggregated information is returned [13]. This kind of nodes in the sensor network, called aggregators, it can collect the raw information from the sensors, process it locally, and reply to the aggregate queries of a remote user.

Due to physical tampering the sensor nodes and aggregators which are deployed in hostile environment may be compromised. Some sensor nodes may be compromised and sent false values; it will affect the aggregator's result [12]. If the compromised sensor node sent a false value, it is very difficult to find the misbehavior of the nodes, such a detect require some special knowledge. In the multiple levels of data fusion multiple data reports are received [14]. There is a possible time lag between the instances of reception of these multiple data reports.

Each sensor node has to decide on when to begin and finish the process of fusion and also decide how long to wait before the end of the fusion. If the sensor node waits longer time for their fusion, it will receive large number of reports. We focus on the stealthy attack [12] the attacker's aim is to make the base station to accept the false result; here we want to ensure that the base station accepts a true data aggregation report from genuine aggregation.

1.4. Security Goal

Practically the sensor network faces many challenges in the real-world. Most of the applications the sensor nodes are deployed in open environment, so we create the efficient random sampling techniques, the base station to verify the data given by the aggregator is true. If the aggregator and few of the sensor nodes are corrupted, the base station to reject the corrupted aggregator report. To summarize, due to their limited power and shorter communication range, sensor nodes perform in-network data fusion.

- A data fusion node collects the results from multiple nodes.
- It fuses the results with its own based on a decision criterion.
- Sends the fused data to another node/base station.
- Due to their energy constraints, sensors need to perform efficient data fusion to extend the lifetime of the network.
- Lifetime of a sensor network is the number of rounds of data fusion it can perform before the first sensor drains out.

Advantages of Fusion are,

1. Reduces the traffic load.
2. Conserves energy of the sensors.

1.5 Types of Sensor Network Reporting

There are three kind of Reporting Generally used in Sensor Network

- Periodical reporting: Sensor nodes periodically send reports to the base station.
- Base station inquiry response reports: the BS queries sensors in specific regions for current sensed information.
- Event triggered reports: The occurrence of a certain event can trigger reports from sensors in that particular region.

Due to their limited power and shorter communication range, sensor nodes perform in-network data fusion.

- A data fusion node collects the results from multiple nodes.
- It fuses the results with its own based on a decision criterion.
- Sends the fused data to another node/base station.
- Due to their energy constraints, sensors need to perform efficient data fusion to extend the lifetime of the network.
- Lifetime of a sensor network is the number of rounds of data fusion it can perform before the first sensor drains out.
- Advantages of Fusion:

  Reduce the traffic load.

  Conserve energy of the sensors.

Data fusion is most suited for Periodical Reporting scenario and Event Driven Reporting scenario. In this project a Periodical reporting Scenario may be under consideration

Previously, it is assumed that the nodes conducting the data fusion are secured. But, a malicious data fusion node can send bogus reports to the BS. The BS is incapable of detecting the bogus information since the sensor nodes do not directly send the reports to the BS. This project addresses a novel power efficient data fusion assurance scheme for sensor network using silent negative voting mechanism.

1.6 Fusion Architectures

There are three kinds of Fusion architectures generally used

1. Centralized:

- Simplest Method
- A central processor fuses the reports collected by all other sensing nodes.
- Advantage: Erroneous report(s) can be easily detected.
- Disadvantage: inflexible to sensor changes and the workload is concentrated at a single point.

2. Decentralized:

- Data fusion occurs locally at each node on the basis of local observations and the information obtained from neighboring nodes.
- No central processor node.
- Advantages: scalable and tolerant to the addition or loss of sensing nodes or dynamic changes in the network.

3. Hierarchical:

- Nodes are partitioned into hierarchical levels.
- The sensing nodes are at level 0 and the BS at the highest level.
- Reports move from the lower levels to higher ones.

- Advantage: Workload is balanced among nodes

2. PROBLEM SPECIFICATION

The sensor nodes detect the environmental variations and then transmit the detection results to specialized gateway nodes or a centralized base station [9][10][5]. One or more than one sensors collect the data from other sensors. The collected data are processed by the sensor to minimize the transmission load before they are transmitted to the base station. This process is called data fusion [10]. Data fusion, which fuses the collected data before they are sent to the base station, is usually implemented over the network. Since the sensor is typically placed in locations accessible to malicious attackers, information assurance of the data fusion process is very important.

If a fusion node is compromised, then the base station cannot ensure the correctness of the fusion data sent to it. A malicious data fusion node can send bogus reports to the base station. The base station is incapable of detecting the bogus information since the sensor nodes do not directly send the reports to the base station. Various methods are proposed, that deal with providing an assured data transfer to the Base Station.

2.1 Existing Solutions

There are two types of solutions are there, one is hardware-based [11] and the other is software-based [5]. The hardware-based solution requires extra hardware to detect the compromised node, so the cost and power consumption of sensors are increased but still no guarantee protection for all attacks. The software based solution requires no extra hardware for data assurance. Here several copies of the fusion data required to send the base station, so the power consumption for the data transmission is very high.

"Power-Efficient Data Fusion Assurance Using Direct Voting Mechanism in Wireless sensor Network" proposed by Hung-Ta Pai and Y. S. Han [4]. In this work they developed a new data fusion assurance to improve the witness-based method. The correctness of the verification in the proposed scheme depends only on the number of compromised fusion nodes.

2.2 The Proposed Solution

The proposed model will more resemble like Direct Voting Mechanism based approach. In this method also, a fusion node is selected to transmit the fusion result, while other fusion nodes serve as witnesses. But in this case, the witness's nodes will be silent if there are no compromised nodes. If a compromised node is sending false data, then one or more witness's nodes will put a negative vote. Conceptually, it is more efficient and reliable than the previously proposed methods mentioned above.

3. VOTING BASED FUSION ASSURANCE MECHANISM

As in the witness-based approach, a fusion node is selected to transmit the fusion result, while other fusion nodes serve as witnesses. Nevertheless, the base station obtains votes contributing to the transmitted fusion result directly from the witness nodes.

Only one copy of the correct fusion data provided by one uncompromised fusion node is transmitted to the base station. No valid fusion data are available if the transmitted fusion data are not approved by a pre-set number of witness nodes. Analytical and simulation results reveal that the proposed scheme is up to 40 times better on the overhead than that of the witness based approach.

The voting mechanism in the witness-based approach is designed according to the MAC of the fusion result at each witness node. This design is reasonable when the witness node does not know about the fusion result at the chosen node. However, in practice, the witness node is in the communication range of the chosen node and the base station, and therefore can overhear the transmitted fusion result from the chosen node. The witness node then can compare the overheard result with its own fusion result.

Finally, the witness node can transmit its vote (agreement or disagreement) on the overheard result directly to the base station, rather than through the chosen node. The base station has to set up a group key for all fusion nodes to ensure that the direct voting mechanism works.

When a fusion node wishes to send its fusion result to the base station, it adopts the group key to encrypt the result, and other fusion nodes serving as witness nodes can decode the encrypted result. The witness node then starts to vote on the transmitted result.

A Polling Scheme based on the voting mechanism using a public key was proposed to ensure data fusion assurance.

3.1 Pros & Cons of Witness Based Data Assurance Algorithm

- Pros : Provides a scheme that ensures that only valid reports are accepted by the BS in an efficient manner.
- Cons : Polling Scheme is an overhead. Use of a public key is a threat to security.

4. DATA FUSION ASSURANCE USING SILENT NEGATIVE VOTING

As in the Direct Voting Mechanism based approach, a fusion node is selected to transmit the fusion result, while other fusion nodes serve as witnesses. But in this case, witness's nodes will be silent if there are no compromised nodes. If a compromised node is sending false data, then one or more witness's nodes will put a negative vote.

- In the proposed method, a fusion node is randomly selected for forwarding the fusion data as in the previous methods. But, instead of sending the data, the fusion node will send a MAC (Message Authentication Code) by encrypting it with its private key provided by the BS.
- The BS will receive the encrypted MAC and decrypt it with the private key of the selected Fusion Node.
- The BS will broadcast the MAC after encrypting it using a Public key or Group key and wait for Negative votes from the fusion nodes which will not compromise with the MAC.
- All the Fusion nodes will receive the Encrypted MAC given by BS and calculate another MAC using the locally available Fusion Data and compare it with the Decrypted copy of Received MAC.
- If the Received MAC and the newly created MAC differ, then the fusion node will prepare a Negative-Vote along with newly calculated MAC encrypt it with its private key and pole it to BS.
- If there will not be sufficient Negative-votes from fusion nodes, then the BS will ask the selected Fusion Node for real Fusion Data and receive it.

4.1 Reliability of the Proposed Mechanism

- In this proposed mechanism, virtually there will not be any need for retransmission of fusion data until the randomly selected fusion node was a malicious node.
- If a malicious Fusion node tries to do Negative voting to invalidate the fusion data of some other selected fusion node, then it will not be considered at the BS since there will not be sufficient Negative Votes from other Genuine Fusion Nodes.
- Since a Private Key is used for Negative voting, the malicious fusion node even can not pole any proxy Negative-votes also.
- If a malicious fusion node will be selected by BS then it may try to send valid MAC to got approval from BS and will send invalid Fusion Data. If it is the case then it can be detected at BS just re-calculating the MAC and comparing it with the previously sent MAC of the malicious node.
- If it will try to send invalid MAC to BS, then BS will receive a lot of Negative-Votes from other genuine Fusion Nodes and will neglect the Malicious Node.

4.2 Advantages of the Proposed Mechanism.

- Since small size MAC is only used to validate the data, and only one time it is transmitted from one selected fusion node to BS, the power will be preserved at other fusion nodes.
- Since the Fusion Data transmission will consume lot of power, obviously the proposed method will preserve lot of transmission power by avoiding retransmission.
- Since Negative-voting mechanism is used, the power will be used for Negative-voting if and only if there is a invalid MAC at BS. So the power at the Fusion nodes will not be wasted for voting/Negative-voting during normal operations.

5. THE SIMULATION AND ANALYSIS

5.1 Hierarchical Fusion Architecture

The problem dealing in this project is related with the hierarchical fusion Architecture where security is the major concern.

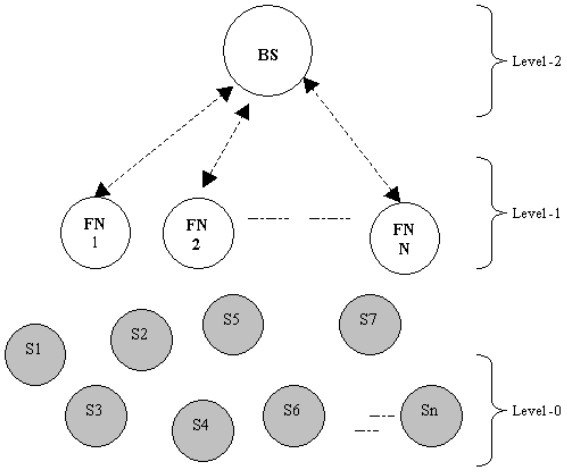

Figure 1 : The Hierarchical Fusion Architecture

In a practical sensor network, the 0th Level May contain many normal Sensors organized in a topographical area, and to minimize the transmission power, the data from individual sensor nodes will be forwarded to all the distant fusion nodes by adopting a suitable routing algorithm. And to minimize the transmission power, the data of a sensor node can be forwarded to a fusion node through the nearby sensor nodes using a routing algorithm like directed diffusion or simple flooding.

For the purpose of comparison, along with the proposed scheme, two other algorithms were implemented. The first algorithm used for comparison is a normal and very common fusion assurance scheme based on Message Authentication Code (MAC). The second algorithm used for comparison is an implementation of previous work "Direct Voting Based Fusion Assurance". The proposed algorithm "Fusion Assurance using Silent Negative Voting" will be compared with the other two.

So the Algorithms going to be implemented on ns2 are :

1. Direct Voting Based Fusion Assurance
2. Fusion Assurance using Silent Negative Voting

5.2 The Simulation Setup

The Power Efficient Data Fusion Assurance scheme dealing in this paper is related with the hierarchical fusion Architecture. So a hierarchical sensor network will be simulated. In the simulated sensor network, there will be three levels of nodes.

- In the 0th Level, there will be N normal sensor nodes which will collect all the local sensor data and forward periodically to all the next level fusion nodes.
- In the 1st Level, there will be M Fusion nodes which will fuse the data collected from the 0th Level sensors and send the fused data to a higher level base BS (Base Station) on the request from the BS.
- The Valid Fusion Data will be available on BS which is at topmost level (2nd level) in this architecture according to the adopted Data Fusion Assurance scheme.

Assumptions:

- The address of the fusion nodes may be resolved by simple periodic hello broadcast from the Fusion Nodes or the address may be internally coded in the sensor hardware it self and hence the low level sensor nodes can periodically forward the local data to all the Fusion nodes.
- If there will be more than one Layer of Normal Data collecting Sensors at 0th level, then the routes of the Fusion nodes will be resolved by adopting suitable routing protocol at 0th Level.
- Every fusion node must correctly fuse all of the local data and the fusion results should be same. This work assumes this problem has been solved. For this we are going to simulate and use same dummy fusion data at all the fusion nodes except the compromised nodes and randomly simulate wrong fusion data in the compromised fusion nodes (malicious nodes) to simulate attack.

5.3 Experimental Setup

We have used the directed diffusion code in NS-2 implemented by USC/ISI[1] and mobility extensions that were implemented by the CMU Monarch project [2]. For our simulations, we use a sensor network comprising of 1 Base Station(BS), 5 Fusion Sensor(FS) nodes and 20 Normal Sensor Nodes (SN)

which are dispersed on a topographical are to form a network with hierarchical fusion architecture.

Since "Energy Model" of ns2 is used to analyze the energy consumption of the nodes, the following energy related parameters were used while creating the node

Initial Node Energy : 1000 Joules

The txPower of a Node : 4.5099 Watts

The rxPower of a Node : 0.430 Watts

The Idle Power of a Node : 0.030 Watts

A Dummy Data size of 1024 bytes is used to represent the fused data and the size of Message Authentication Code (MAC) was assumed as 64 bytes.

Since the simulation was run for small duration, the fusion assurance session interval was set as 5 seconds. To simulate attack, false votes were polled with probability of 0.2. (That is, for each 100 votes, 20 % of the votes will be polled wrongly to simulate attack)

5.4 The Simulation Results

The following graph shows the average power consumption at fusion nodes and the base station.

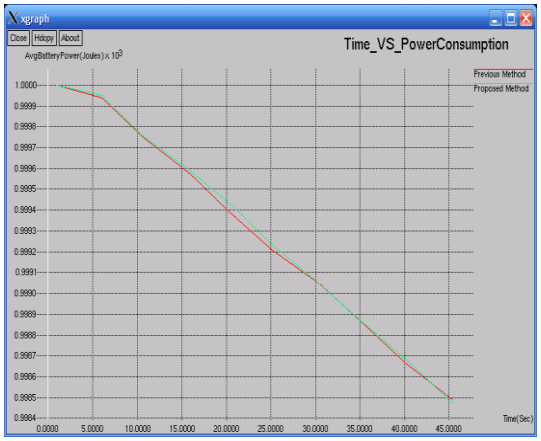

Figure 2: The Power Consumption

As shown in the above graph, the poer consumption during data fusion assurance in the case of proposed method is little bit lower than the direct voting based method.

The following graph measures the overhead in terms of total sent and received packets at the fusion nodes and the base station.

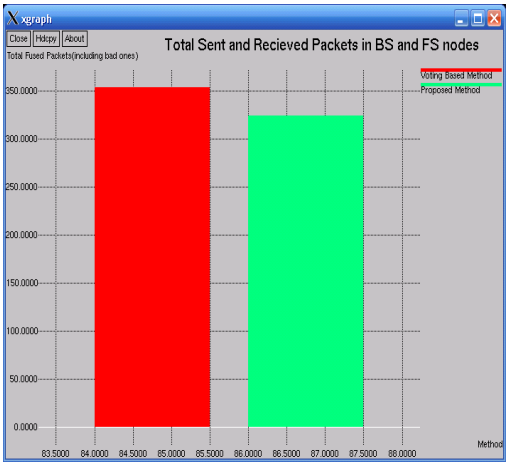

Figure 3: The Overhead in Terms of Received Packets

The following graph measures the overhead in terms of total sent and received bytes at the fusion nodes and the base station.

Figure 4: The Overhead in Terms of Received Bytes

As shown in the above chart, the overhead in terms of total sent and received bytes at the fusion nodes and the base station in the proposed method is almost equal to that of direct voting based method (But in the proposed method, the overhead is little bit lower).

6. CONCLUSION AND FUTURE WORK

We have successfully Implemented and evaluated two different models for data fusion assurance under ns2. It was found that, among the two evaluated algorithms, namely 1. Direct Voting Based Method, and 2. The proposed "Fusion assurance using Silent negative votes", the Second one is the best performer.

The arrived results were significant and more comparable. The arrived results prove that the proposed scheme will improve the performance of the fusion and increase the network life time considerably.

In future works, we may consider the individual node's power during the selection of the fusion node. If we select the node which is having high battery power for fusion assurance, then naturally, it will extend the life of the whole network. The issues related with such more power aware models can be addressed in future works

7. ACKNOWLEDGEMENT

We thank our Management who gave the opportunity to do the research works in this institution. I would like to thank our principal who motivated me and provided the facilities and resources to do my research work. Thus I prepared this paper successfully.

REFERENCES

[1]. "Ns-2 network simulator," http://www.isi.edu/nsnam/ns/, 1998.

[2]. "CMU Monarch extensions to ns-2," http://www.monarch.cs.cmu.edu/cmu-ns.html, 1999.

[3]. Marc Greis' Tutorial for the UCB/LBNL/VINT Network Simulator "ns"

[4]. Hung-Ta Pai and Yunghsiang S. Han , July 2006 , Power-Efficient Data fusion Assurance Using Direct Voting Mechanism in Wireless Sensor Networks, Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06) .

[5]. W. Du, J. Deng, Y. S. Han, and P. K. Varshney. A Witness-Based Approach For Data Fusion Assurance In Wireless Sensor Networks. In Proc. GLOBECOM 2003, volume 3, pages 1435–1439, San Francisco, CA, Dec. 2003.

[6]. A.Sinha and A.Chandrasekar, Dynamic , Power management in wireless sensor network, IEEE Design and test of Computer" pp 62-74 march-April 2001.

[7]. I.F.Akyildiz, W.Su, Y.Sankarasubramanian , E.Cayirai, A Survey an sensor network , IEEE Commun, May 40(8)(2002).

[8]. Suat ozdemir, Yanaxiao, Secure data aggregation in wireless sensor networks ; A Comprehensive overview , Elsevier Computer Networks 53 (2009) 2022-2037.

[9]. S.A.Aldosai and J.M.F.Moura, Detection in Decentralized Sensor Networks, Proc Intil Conf. Acoustics, Speech, and signal processing, pp. 277-280 may 2004.

[10]. Hung-Ta pai, and Yunghsiang S.han, Power-Efficient Direct-voting Assurance for Data Fusion in Wireless Sensor Networks, IEEE Transaction on Computer Vol 57 No 2 Feb 2008.

[11]. R.Andersan and M.Kuhn, Tamper Resistance – A Cautionary Note , Proc. Second usenix workshop Electraonic Commerce, pp 1-11, nov 1996.

[12]. Bartosz Przydatek, Dawn Song, Adrian Perrig, SIA : Secure Information aggregation in Sensor Networks, Journal of Computer Society Vol 15 Issue 1 January 2007 special issue on security of Ad-hoc and Sensor networks pp 69-102, January 2007.

[13]. C.Intanagonwiwat, D Estrin, R.Govindan, and J.Heidemann. Impact of network density on data aggregation in wireless sensor networks. In Proc International conference on Distributed Computing Systems, November 2001.

[14]. Wei Yuan, Srikanth V.Krishnamurthy, and Satish K. Tripathi, Synchronization of Multiple Levels of Data Fusion in Wireless Sensor Networks, Proc IEEE Global Telecommunication conference, 2003 GlobeCom'03 vol 1 pp 221-225.