World Applied Sciences Journal 29 (Computer Sciences, Engineering and Its Applications): 42-47, 2014
ISSN 1818-4952
© IDOSI Publications, 2014
DOI: 10.5829/idosi.wasj.2014.29.csea.2218

Power-Efficient Data Fusion Assurance Using Indirect Anti-Voting Mechanism in Wireless Sensor Networks

R. Udayakumar, K.P. Thooyamani Khanaa and A.V. Allin Geo

School of Computing Science, Bharath University, Chennai - 73, India

Abstract: In Wireless sensor networks (WSNs), the sensors detect environmental variations and then transmit the detection results to other sensors or a Base Station. The collected data must be processed by some sensors, so as to reduce the transmission burden before transmitting the data to the Base Station. This process is called Data Fusion and the sensors performing data fusion are the fusion nodes. Although fusion significantly lowers the traffic between the fusion nodes and the Base Station, the fusion nodes are more critical and vulnerable to malicious attacks than non-fusion sensors. If a fusion node is compromised, then the Base Station cannot ensure the correctness of the fusion data sent to it. This work focuses on providing data fusion assurance, power efficiently. The new method portrayed here is the Indirect Anti-Voting Mechanism. A fusion node is selected at random for forwarding the fusion data as in the previous methods. But instead of sending the data, the fusion node sends an encrypted aggregate value to the Base Station. The Base Station decrypts and broadcasts the aggregate and waits for Anti-Votes from the fusion nodes which do not comply with the fusion result.

Key words: Data Fusion · Malicious node · Direct Voting · Aggregate · Indirect Anti-Voting

INTRODUCTION

Recent advances in electronic and computer technologies have paved the way for the proliferation of ubiquitous wireless networks. Fast deployment of communication networks is highly desirable under many situations, such as establishing efficient, survivable dynamic communications for emergency and rescue operations. While the Base Station can have continuous, unlimited power supply, the sensor nodes usually have limited power supply and are battery-powered [1]. It is inconvenient to replace once deployed in the field. Sometimes, replacement is even impossible. Thus energy efficiency is a critical design consideration of wireless sensor networks. In these networks, communication is a dominant source of energy consumption [2].

The aim is efficient transmission of all the data to the Base Station so that the lifetime of the network is maximized in terms of *rounds*, where a round is defined as the process of gathering all the data from sensor nodes to the Base Station, regardless of how much time it takes [3]. Direct transmission, a simple approach for this problem in which each node transmits its own data directly to the Base Station. However, if the Base Station is far away, the cost of sending data to it becomes too large and the nodes die quickly. Since large number of sensor nodes are densely deployed, neighbour nodes may be very close to each other. Multihop communication can effectively overcome some of the signal propagation effects experienced in long-distance wireless communication. Sensor nodes carry limited, generally irreplaceable, power sources. Therefore, while traditional networks aim to achieve high quality of service (QoS) provisions, sensor network protocols must focus primarily on power conservation [4]. By avoiding unnecessary transmissions, power consumption in a wireless sensor network can be very much reduced. This is made possible by Data Fusion. Data Fusion is the collection and processing of information from various sensors, before transmitting it to the Base Station, thereby reducing the amount of traffic. The data from a group of sensors (referred to as clusters) are collected at their corresponding clusterheads or fusion nodes. These fused data from the clusterheads are then transmitted either to the other clusterheads or sent to the

Corresponding Author: R. Udayakumar, School of Computing Science, Bharath University, Chennai - 73, India.

command center (Base Station). The sensors do not communicate with one another, but the clusterheads can communicate with the other clusterheads. Thus, sensors and clusterheads are functionally different.

Thus data Fusion reduces the traffic load, conserves energy of the sensors and reduces the redundancy in the data at the Base Station [5, 6]. Even though this data collection and processing architecture drastically relieve the communication burden on the network, the nodes conducting data fusion are vulnerable to attacks. Data fusion 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 data fusion node is compromised, it can send bogus data to the Base Station. In particular, we want to guarantee that if the Base Station accepts a reported fusion result from the fusion nodes, then the reported result is "close" to the true value with high probability.

Communication bandwidth is extremely dear: each bit transmitted consumes about as much power as executing 800–1000 instructions [7] and as a consequence, any message expansion caused by security mechanisms comes at a significant cost. Thus, the resource-starved nature of sensor networks poses great challenges for security. In a sensor network, an adversary can easily inject messages, so the receiver needs to make sure that the data used in any decision-making process, originates from the correct source. Data authentication prevents unauthorized parties from participating in the network and legitimate nodes should be able to detect messages from unauthorized nodes and reject them. In the two-party communication case, data authentication can be achieved through a purely symmetric mechanism: The sender and the receiver share a secret key to compute a Message Authentication Code (MAC) of all communicated data. When a message with a correct MAC arrives, the receiver knows that it must have been sent by the sender. Once an incorrect MAC is detected, that report is dropped [8]. Various methods have been proposed that deal with providing an assured data transfer to the Base Station. They are Witness Based Approach and Direct Voting. But these methods have various demerits. A brief overview of these methods is given below.

Information Assurance: The fusion nodes can combine all of the local decisions to yield a final result and directly communicate with the Base Station. Finally, one of the fusion nodes is specified to send the final result to the Base Station. Unless all the fusion nodes or all the sensors fail, this detection and fusion scheme guarantees that the Base Station obtains the detection result. However, the accuracy of the result is not certain. Two problems must be solved to ensure that the Base Station obtains the correct result. First, every fusion node must correctly fuse all the local decisions, which also implies that all the fusion results must be the same. This work assumes that this problem has been solved. The second problem is concerned with the assurance of the fusion result. The transmission between the fusion node and the Base Station is assumed herein to be error-free. Since some fusion nodes may be compromised, the fusion node chosen by the Base Station to transmit the fusion result may be one of the compromised nodes. Malicious data may be sent by the compromised node and the Base Station cannot discover the compromised nodes from the normal fusion nodes, since the data detected by the sensors are not sent directly to the Base Station. Consequently, the result obtained at the Base Station may be incorrect [9].

Existing System

Witness Based Approach: Du *et al*. [10] used the "witness" concept to solve the assurance problem between data fusion nodes and the Base Station. Du *et al.* presented a Witness Based Approach to ensure the correctness of the fusion result. One of the fusion node is chosen to transmit the fusion result to the Base Station All the other fusion nodes, act as witnesses of the transmitted fusion result. Several fusion nodes are used to fuse the collected data and have the ability to communicate with the Base Station. Witnesses, encrypt the fusion results to Message Authentication Codes (MACs). (Figure 1) The MACs are then sent to the Base Station through the chosen fusion node. Finally, the Base Station utilizes the received MACs to verify the received fusion data. A long MAC increases the reliability of the verification. However, the transmission of the long MAC imposes a high communication burden. If the received fusion result at the Base Station cannot pass the verification, then a polling scheme is started to determine whether any valid fusion result is available at the other fusion nodes.

Demerits:

Long MAC′s are an overhead
Many copies of the fused data are sent to the Base Station. Not Power efficient.

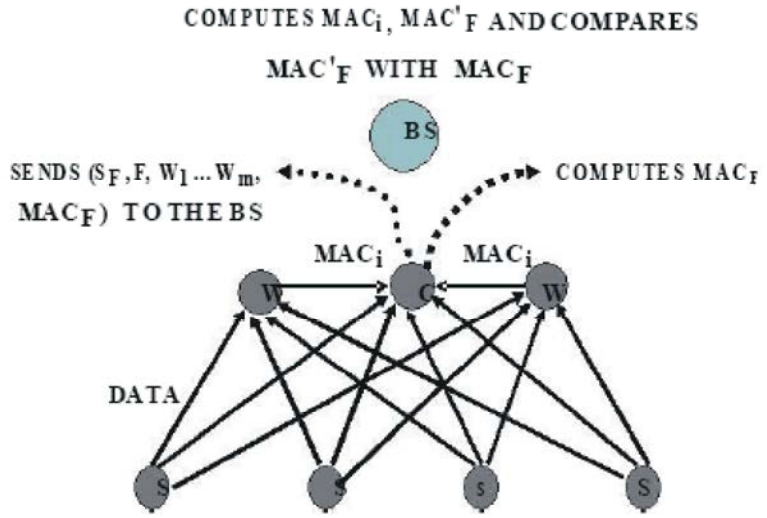

Fig. 1: The Witness Based Approach

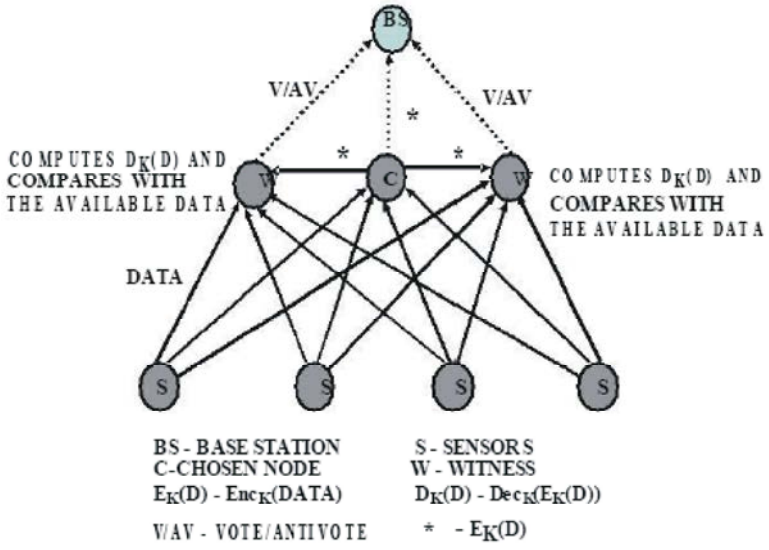

Fig. 2: Direct Voting

Direct Voting Mechanism: Hung-Ta Pai and Yunghsiang S. Han [9] proposed a new scheme to ensure data fusion assurance. This method is better than the witness-based method (Figure 2). 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. The witness node overhears the transmitted fusion result from the chosen node. It then compares the overheard result with its own fusion result. Finally, the witness node can transmit its vote on the overheard result directly to the Base Station, rather than through the chosen node. 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 is proposed to ensure data fusion assurance.

Demerits: The Polling Scheme is an overhead.
Use of a public key is a threat to security.

Proposed System: This work proposes a novel Power-Efficient Data Fusion Assurance Using Indirect

Anti-Voting Mechanism. If several copies of the fusion data are sent to the Base Station, power consumption for data transmission is very high. Hence in this method, instead of sending the entire set of fused data, only the aggregated value of the data collected is transmitted to the Base Station. The proposed mechanism adopts the public-key cryptography [7]. The method makes use of set of keys as discussed below. In the proposed method, a fusion node is selected at random for forwarding the fusion data as in the previous methods. But, instead of sending the data, the fusion node sends an aggregate value to the Base Station, by encrypting it with the K_1, where

K_1 = private key of the fusion node+ public key of the Base Station (3.1)

Data after encryption = data from the sender ^ K_1 (3.2)

- The Base Station receives the encrypted value, decrypts it with key K_2, where

K_2 = private key of the Base Station + public key of the Fusion node (3.3)

Data after decryption at the receiver = data at the receiver ^ K_2 (3.4)

- The Base Station broadcasts the aggregate value after encrypting it with a key K2
- The Base Station waits for Anti-Votes from the fusion nodes which do not accept the fusion result.
- All the fusion nodes receive the encrypted aggregate value sent by the Base Station. They calculate another aggregate, using the locally available fusion data and compare it with the decrypted copy of the received aggregate. Here decryption makes use of a key K_1.
- If the aggregate values differ, then the fusion nodes prepare Anti-Votes, encrypt them with key K_1 and pole it to the Base Station.
- If there are no sufficient Anti-votes from the fusion nodes, then the Base Station requests the selected Fusion Node for real fusion result and then receives it.

Credibility 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 is a malicious node. As the fusion node to transmit the data is selected at random, the intruder will not be able to find out the node chosen at that particular instant. Hence the vulnerability of attacks is very much reduced. If a malicious fusion node generates Anti-votes to invalidate the data of some other fusion node chosen to forward the data, then it will not be considered at the Base Station, as there will not be sufficient Anti-votes from other genuine fusion nodes to support this node [6, 11]. Since a public-key system is used, a malicious fusion node cannot pole any proxy Anti-votes also. The main merit is that the private keys are not communicated, transmitted or revealed to any other nodes. If the malicious node tries to send invalid aggregate to the Base Station, the Base Station receives a lot of Anti-Votes from other genuine fusion nodes and rejects the malicious node. The malicious fusion node may try to send a valid aggregate to get approval from the Base Station and then send an invalid fusion data. If this is the case, this can be detected at the Base Station by re-calculating the aggregate and comparing it with the one sent already by the same malicious node. This is shown pictorially in Figure 3.

Performance Analysis: The system was simulated using ns2. The following graphs the reduction in transmission overhead, conserves energy.

Reduced Power Consumption in the Proposed Mechanism: An aggregate very small in size is used to validate the data. It is transmitted only once from the selected fusion node to the Base Station. Power is preserved at the other fusion nodes. In the Witness Based Approach, many copies of the fusion data (MAC) are sent to the Base Station and in the Direct Voting Mechanism one encrypted copy of the fusion data is made available at the Base Station. In the existing methods this copy of the data has to be approved by other witness nodes. Only then will the Base Station accept the fusion data [12, 13]. In case the Base Station rejects the data, copy/copies of the fusion data at the Base Station is a transmission overhead. In this proposed method, this is avoided by initially sending the aggregate value to the Base Station and then sending the fusion data only when the Base Station makes a request. Since the transmission of fusion data consumes a lot of energy, obviously the proposed method reduces the transmission overhead and thereby power consumption. This system avoids re-transmission also. Since Anti-Voting mechanism is used, power is spent only for Anti-voting, (i.e) if and

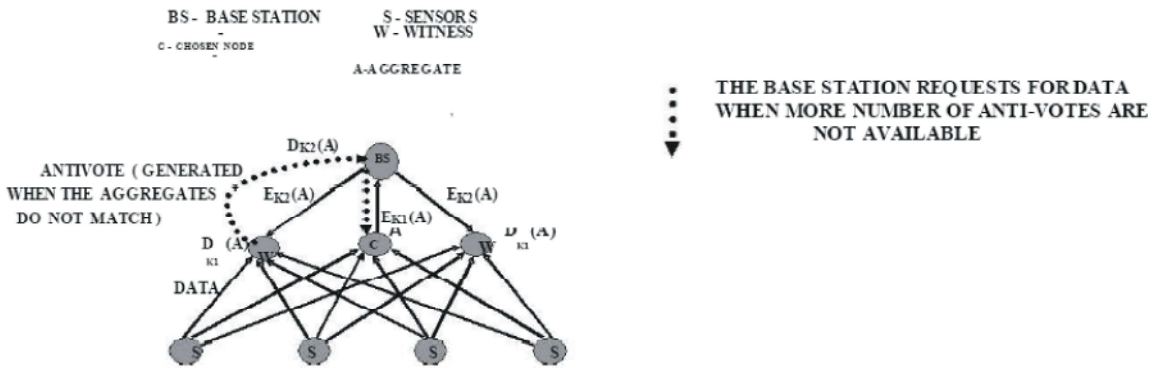

Fig. 3: Indirect Voting

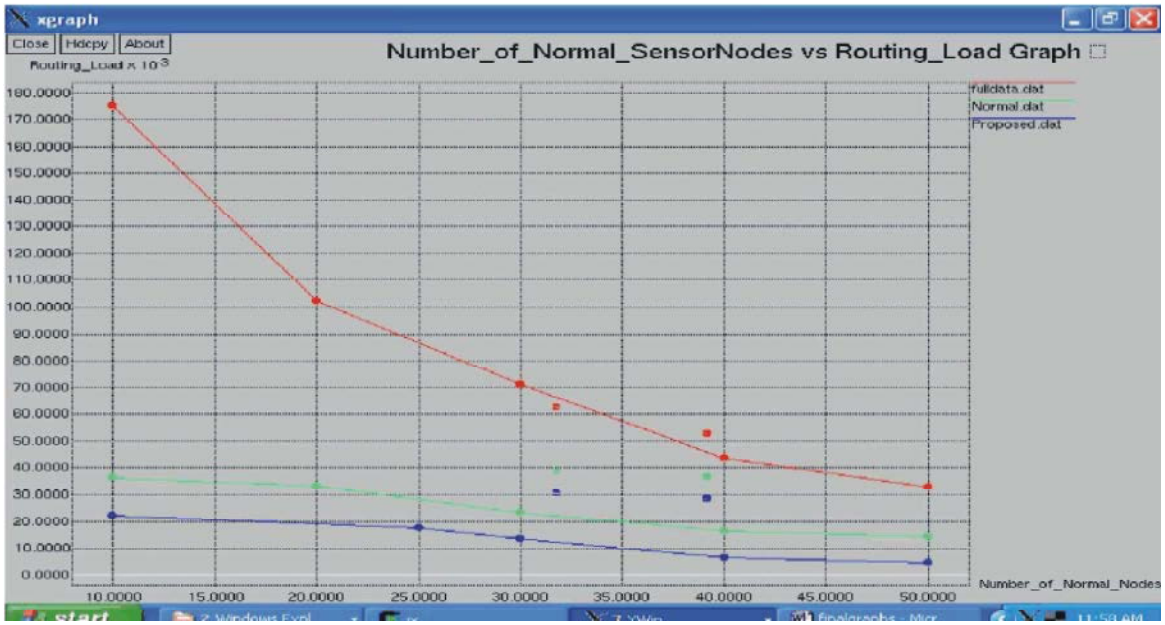

Fig. 4: Graph showing the transmission load (1) when the fusion data, anti-votes and votes are sent (2) when the aggregate and both anti-votes and votes are sent (3) when the aggregate and only anti-votes are sent

only if there is an invalid aggregate at the Base Station. So the power at the Fusion nodes is not wasted for Voting/Anti-Voting during normal operations.

CONCLUSION

Power consumption plays a vital role in wireless sensor networks. So this work conserves power to a greater extent by reducing the unnecessary transmissions. The amount of traffic in the network is very much reduced as only the aggregate value is transmitted instead of the entire set of the fusion data. Only on request by the Base Station will the fusion data be sent to it. Further only Anti-votes are sent. Further to avoid the compromise of the fusion nodes each node has its own private and a public key. Here the keys are not transmitted in the network. So the attacks and the corruption of the keys are avoided. To crown it all, this proposed method provides a secured transfer of data as well as avoids re-transmission.

ACKNOWLEDGEMENT

I thank the Almighty for having given me knowledge to carry out this work. I am indebted to Mrs.Amutha Venkatessh for her valuable guidance and support.

REFERENCES

1. Bartosz, Przydatek and Adrian, Perrig, 2003. SIA: Secure Information Aggregation in Sensor Networks, SenSys'03, Copyright 2003 ACM, USA.

2. Xueyan Tang, Jianliang Xu, Extending Network Lifetime for Precision-Constrained Data Aggregation in Wireless Sensor Networks, partially supported by a grant from the Research Grants Council of the Hong Kong SAR, China (Project No. HKBU 2115/05E).
3. Huseyin Ozgur Tan and Ibrahim Korpeoglu, 2002. Power Efficient Data Gathering and Aggregation in Wireless Sensor Networks, SIGMOD Record, 32(4).
4. Akyildiz, I.F., W. Su, Y. Sankarasubramaniam and E. Cayirci, Wireless Sensor Networks: a survey, Computer Networks, 38: 393-422.
5. Yi Yang, Xinran Wang, Sencun Zhu and Guohong Cao, 2006. SDAP: A Secure Hop by Hop Data Aggregation Protocol for Sensor Networks, MobiHoc'06, Italy.
6. Saravanan, T. and R. Udayakumar, 2013. Optimization of Machining Hybrid Metal matrix Composites using desirability analysis, Middle-East Journal of Scientific Research, ISSN:1990-9233, 15(12): 1691-1697.
7. Hill, J., R. Szewczyk, A. Woo, S. Hollar, D. Culler and K. Pister, 2000. System architecture directions for networked sensors, In Proceedings of ACM ASPLOS IX.
8. Feng Li and Jie Wu, 2006. A Probabilistic Voting-based Filtering Scheme in Wireless Sensor Networks, IWCMC'06, Canada.
9. Hung-Ta Pai and Yunghsiang S. Han, 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).
10. Du, W., J. Deng, Y.S. Han and P.K. Varshney, 2003. A Witness-Based Approach For Data Fusion Assurance In Wireless Sensor Networks, In Proc. GLOBECOM 2003, 3: 1435-1439.
11. Saravanan, T., V. Srinivasan and R. Udayakumar, 2013. Images segmentation via Gradient watershed hierarchies and Fast region merging, Middle-East Journal of Scientific Research, ISSN:1990-9233, 15(12): 1680-1683.
12. Saravanan, T., V. Srinivasan and R. Udayakumar, 2013. A Approach for Visualization of Atherosclerosis in Coronary Artery, Middle-East Journal of Scientific Research, ISSN:1990-9233, 18(12): 1713-1717.
13. Udayakumar, R., V. Khanna, T. Saravanan, G. Saritha, 2013. Retinal Image Analysis Using Curvelet Transform and Multistructure Elements Morphology by Reconstruction, Middle-East Journal of Scientific Research, ISSN:1990-9233, 16(12): 1798-1800.
00. Udayakumar, R., V. Khanna, . Saravanan, G. Saritha, 2013. Cross Layer Optimization For Wireless Network (Wimax), Middle-East Journal of Scientific Research, ISSN:1990-9233, 16(12): 1786-1789.
00. Saravanan, T. and R. Udayakumar, 2013. Comparision of Different Digital Image watemarking techniques, Middle-East Journal of Scientific Research, ISSN:1990-9233, 15(12): 1684-1690.