ISSN No. 0976-5697

Volume 5, No. 5, May-June 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Power Efficient Data Fusion Assurance Mechanism for Wireless Sensor Networking

M. Umashankar
Department of Computer Applications, Sona College of Technology,
Salem, Tamilnadu, India

Abstract: The low power wireless sensor networks need both security and efficiency to collect sensitive data from various nodes.. Data fusion nodes fuse the collected data from nearby sensor nodes before they sent to the base station. If a fusion node is compromised, then the base station cannot ensure the correctness of the fusion data. Several 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 witness based fusion assurance scheme as well as the direct voting based fusion assurance scheme. The proposed scheme has produced very good impact with better power efficiency and lower network overhead.

Keywords: Wireless Sensor Network, Data Fusion, Fusion Assurance, Network security, voting.

I. INTRODUCTION

Wireless sensor networks (WSNs) consist of inexpensive sensor nodes, each node has continuous sensing capability with limited communication power [1]. 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 with inbuilt chips and software are used for processing specific function. The security application of a wireless sensor network is to collect and analyze data remotely and to detect any kind of attack. In military applications, a wireless sensor network is used to collect sensitive data, and such passed over information must be very secure. However, sensor networks are relatively more insecure repository and routers of data, which increases the need of new security schemes. Their deployment in environmental 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. Securing data streams in sensor networks are important because traditional encryption and authentication protocols such as TinySec are often unable to keep up with high stream rates, and they deplete the network of energy too quickly [2]. The authors in [3] propose a one-time pad for confidential transmission of data messages.

Sensor nodes are self-powered and equipped with low computational power CPU allowing the sensor to execute a specific processing before sending a report to the centralized authority. The amount of power carried by the sensor itself is very limited; replacing the sensor or sensor battery is a very time consuming and costly process, in certain application environment. Therefore, the energy saving mechanism is an important issue for research in wireless sensor network [4]. The sensor nodes detect the environmental variations and, then transmit the detection results to specialized gateway nodes or a centralized base station. 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 [5]. 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. There are two types of solutions namely hardware-based [6] and software-based [7]. The hardware-based solution requires extra hardware to detect the compromised node, so the cost and power consumption of sensors are increased. The software based solution requires no extra hardware for data assurance. There are two methods discussed. Witness based method by[7]. This method ensured that the BS accepts only valid data fusion results. To prove the validity of a report, the fusion node is required to provide proof from several witnesses. Direct voting mechanism by [8] developed a new data fusion assurance to improve the witness-based method.

The rest of this paper is organized as follows. Section II introduces the concept of data fusion and the assurance of data fusion nodes. Section III briefly describes the related works. The proposed method is presented in Section IV. Simulation and analysis are summarized in Section V. While Section VI presents the conclusion.

II. DATA FUSION

The wireless sensor network consists of several sensor nodes, because a single sensor is not sufficient for the compensation and correction of 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 environmental 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 advancements 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 to design and develop a perfect information processing and aggregation techniques to make effective use of the aggregate data [9]. Information should be processed and aggregated within the network and aggregated information is returned [10]. 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 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. If the compromised sensor node sent a false value, it will be very difficult to find the misbehavior of the nodes, such detection requires some special knowledge. In the multiple levels of data fusion, multiple data reports are received. There is a possible time lag between the instances of reception of these multiple data reports. Each sensor node has to decide when to begin and finish the process of fusion and also to decide how long to wait. If the sensor nodes wait a longer time for their fusion, it will receive a large number of reports. We focus on the stealthy attack, 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 fusion report from a genuine fusion node.

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

III. RELATED WORKS

Several papers have proposed secure and energy efficient data collection from sensor nodes to base station. In this section, a brief overview of two related approaches of energy efficient and secured fusion assurance mechanisms is provided.

A. Witness Based Fusion Assurance Mechanism:

The witness based approach is to ensure the validity of the data fusion result; the fusion node has to produce the proofs from several witnesses. Each witness computes the Message Authentication Code (MAC) of the result, and then, provides it to the data fusion nodes, who must forward the results to the base station. If the data fusion node is compromised, and wants to send an invalid fusion result to the base station, it will forge the proofs on the invalid result. They assume that the fusion node and witness nodes share a secret key with the base station. After receiving the data from the sensor nodes, each witness conducts data fusion and obtains the result, and then it sends MAC to the fusion node. They use the n out of m+1 voting scheme to determine the validation of the fusion result. The similar voting scheme is also proposed in [11], but in witness approach to reduce energy consumption and computed the minimum length needed for MAC to achieve a pre-defined level of security.

B. Direct 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 will be 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. Two data fusion assurance schemes are proposed. Variant-round scheme, the base station must ask the witness node to transmit their fusion result whether it agrees or disagrees then the witness node sends its vote to the base station. If the transmitted fusion result is not supported by at least T witness nodes, then the base station may have to select another witness node this process to be repeated until T witness nodes agree with the transmitted fusion result. Another scheme is called a one-round scheme. In this scheme the base station randomly chooses a fusion node; the chosen node transmits its fusion results to the base station. The base station will set the fusion result as the temporary voting result. The base station polls the nodes with the best temporary voting result. The witness node compares its fusion result with the best temporary voting result. If the compromised node always disagrees with the transmitted fusion result, then no forged fusion result will be accepted.

This Scheme enables WSN to collect the fusion results and the votes from the fusion nodes directly. It is more reliable with less assurance overhead and delay than the witness-based approach. That is, the power and delay associated with the transmission of the fusion result and the votes are significantly decreased.

IV. DATA FUSION ASSURANCE MECHANISM USING SILENT NEGATIVE VOTING

The proposed model will more resemble like [8]. In the witness-based [7] was designed according to the MAC of the fusion result at each witness node. The direct voting method, the fusion node will be selected to transmit the fusion result, while other fusion nodes will serve as witnesses if they agree or disagree. In our proposed scheme, the witnesses' nodes will be silent if there is no compromised node. If compromised nodes send any false data, then one or more witnesses' nodes will put a negative vote. Conceptually, it is more efficient and reliable than the previously proposed methods mentioned above.

In the proposed method, a fusion node is randomly selected and asks them to forward the fusion data to the base station, instead of sending the data, the fusion node sends a MAC (Message Authentication Code) by encrypting it with its private key provided by the BS. The BS receives the encrypted MAC and decrypts it with the private key of the selected fusion node. The BS broadcasts the MAC after encrypting it using a public key or group key and waits for negative votes from the fusion nodes which will not compromise with the MAC. All the fusion nodes receive the encrypted MAC broadcast by BS and calculate another MAC use the fusion data which are available locally, 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 which are encrypted with its private key and pole it to BS. If there are no sufficient negative-votes from fusion nodes, then the BS will ask the selected fusion node for real fusion data and receive it.

In the proposed mechanism, virtually no 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 cannot poll any proxy negative-votes also. If a malicious fusion node will be selected by BS, it may try to send valid MAC to get approval from BS, and will send invalid fusion data. It can be detected by BS, just re-calculating the MAC and comparing it with the previously sent MAC. If it tries to send invalid MAC to BS, then BS will receive a lot of negative-votes from other genuine fusion nodes, then their data will not be accepted by BS.

V. THE SIMULATION AND ANALYSIS

A. The Hierarchical Fusion Architecture:

The problem dealing in this paper is related to the hierarchical fusion Architecture.

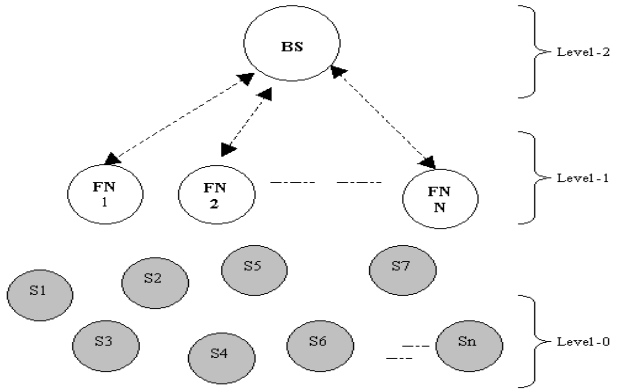

Figure 1: The Hierarchical Fusion Architecture

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 is compared with the other two. The above three algorithms are implemented on ns2.

B. The Simulation Results:

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

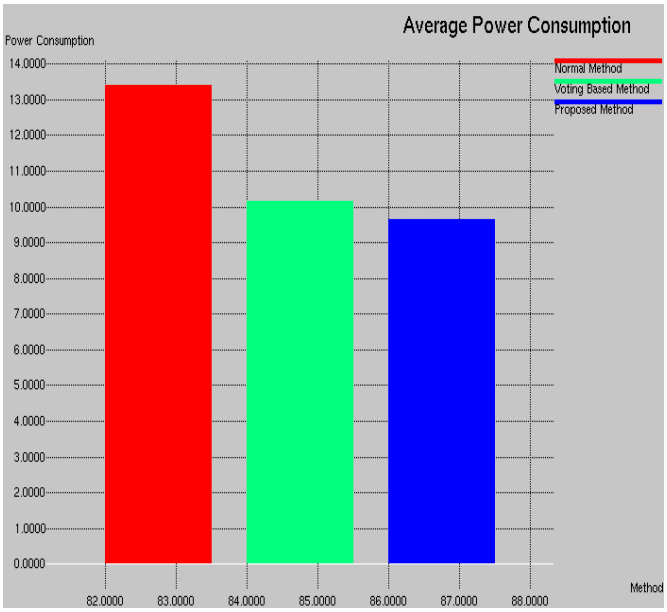

Figure 2: The power consumption

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

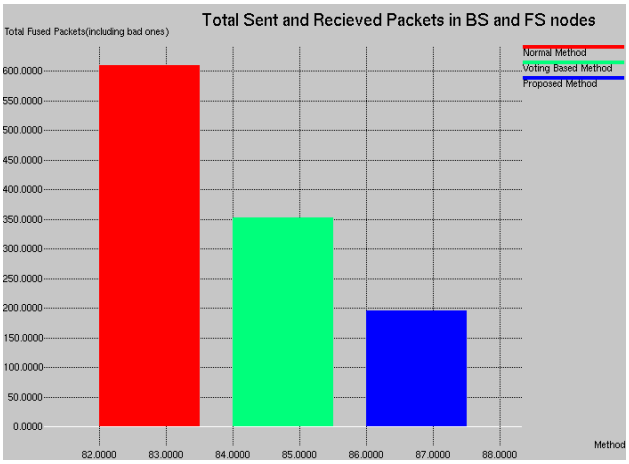

Figure 3: The overhead in terms of received packets.

The above graph shows the overhead in terms of total sent and received packets at the fusion nodes and the base station. It shows the proposed method is very efficient.

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

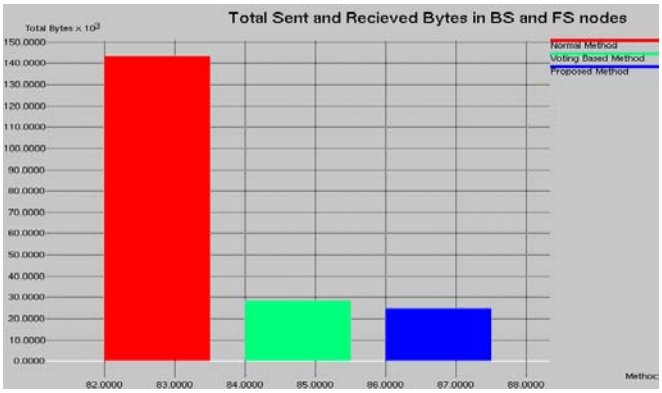

Figure 4: The overhead in terms of receiving bytes

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 a little bit lower) and in the case of normal method, it is very high.

The below graph shown the overhead in terms of routing load at the fusion nodes and the base station. According to the following figure the routing load of the proposed method is considerably low.

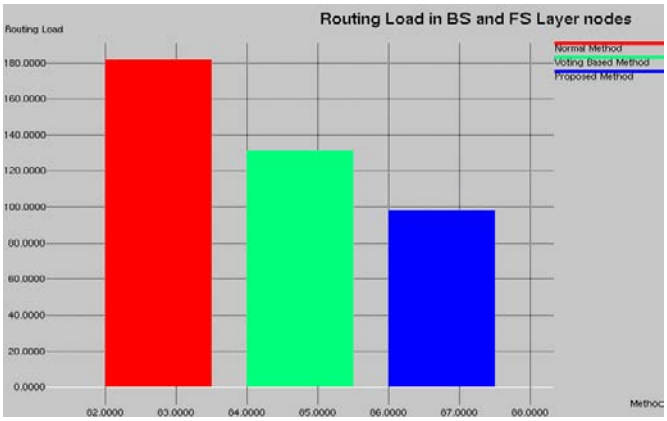

Figure 5: The overhead in terms of routing load

The following graph shows the overhead in terms of dropped packets. If the network is overloaded, then there may be packets drop due to collisions and errors, this will cause the packet drop. So if there is minimum drop, then it will indirectly signify the less over load in the network. Thus our proposed method proves its efficiency.

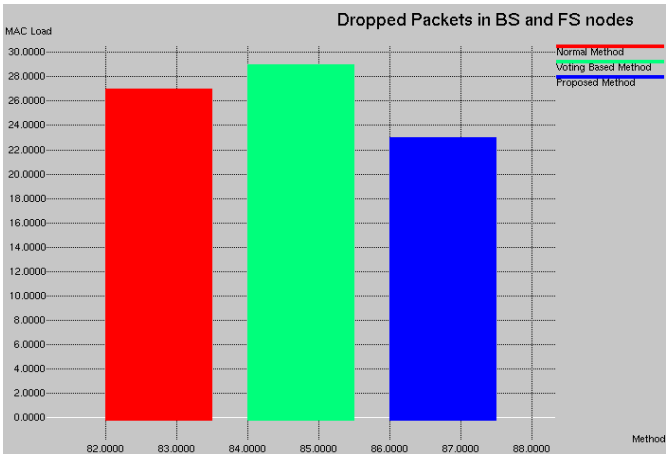

Figure 6: The overhead in terms of dropped packets.

VI. CONCLUSION

This Paper proposes a power efficient mechanism for data fusion assurance. The proposed scheme ensures the validity of the data fusion result and reduces the energy consumption. Witness based approach and direct voting based approach have been analyzed. The proposed scheme with the above two approaches are compared. Arrived results proved that the proposed scheme will improve the performance of the fusion and increase the network lifetime considerably. Future work will 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.

VII. REFERENCES

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

[2]. Karlof, C.,Sastry, N.,Wagner,D.,: TinySec:A link layer security architecture for wireless sensor networks. In; Second ACM Conference on Embedded Networked Sensor Systems (2004) 149-164

[3]. Julia Albath, Sanjay Kumar Madria , Practical algorithm for data security (PADS) in wireless sensor networks. In proceeding of: Sixth ACM International Workshop on Data Engineering for Wireless and Mobile Access, Mobide 2007, Beijing, China. June 10, 2007.

[4]. Wen-Hwa Liao, Hsiao-Hsien Wang, An asynchronous MAC protocol for wireless sensor networks , Journal of Network and Computer Applications 31 (2008)807-820

[5]. Hung-Ta pa, 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.

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

[7]. 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.

[8]. 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) .

[9]. 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.

[10]. 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.

[11]. B. Hardekopf, K. Kwiat, and S. Upadhyaya, "Secure and Fault Tolerant Voting in Distributed Systems," IEEE proc. Aerospace Conf., Vol. 3, pp. 1117-26, 2001

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

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

[14]. 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.

[15]. 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.

[16]. Umashankar M and Chandrasekar C., "Power Efficient Data Fusion Assurance Scheme for Sensor Network Using Silent negative Voting", International journal of Computer Applications, Vol.1, No. 4, pp. 75-80, February - 2010.

[17]. Umashankar M and Chandrasekar C., "Evolution of Power Efficient Data Fusion Assurance Scheme for Wireless sensor Networks", Journal of Theoretical and Applied Information Technology, Vol. 15, No.1, pp. 29-38, May – 2010.

[18]. Umashankar M and Chandrasekar C., "Witness Based And Voting Based Data Fusion Assurance Mechanism In Sensor Networks", International Journal of Research and Review of Applied Science, Vol. 4, No.2 , pp. 194-198, August – 2010.

[19]. Umashankar M and Chandrasekar C., "Energy Efficient Secured Data Fusion Assurance Mechanism For Wireless Sensor Networks", European Journal Of Scientific Research, Vol.49, No.3, pp. 455-463, February – 2011.

