© 2005 - 2010 JATIT. All rights reserved.

EVOLUTION OF POWER EFFICIENT DATA FUSION ASSURANCE SCHEME FOR WIRELESS SENSOR NETWORKS

M.UMASHANKAR[1], DR.C.CHANDRASEKAR[2],

[1] Professor , K.S.Rangasamy College Of Technology, Tiruchengode, Tamilnadu, India

[2] Professor , Periyar University, Salem, Tamilnadu, India

ABSTRACT

Wireless sensor networks processing sensitive data are facing the risks of data manipulation, data fraud and sensor destruction or replacement. However, the practical deployment of sensor networks faces many challenges imposed by real-world demands. Sensors are deployed in open environments, and hence are vulnerable to physical attacks, potentially sensor networks faces many challenges. Security is a very important issue when designing or deploying any network or protocol. In this paper we look at Data fusion process. 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 we present the evaluation of two methods named witnessed based and direct voting. Based on this evaluation here I proposed the new method named silent voting.

Key Words: *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 [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 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.

1.2 System Model

The model of Wireless Sensor Network we have considered here is as follows: The network may be composed of hundreds of sensor nodes. Sensor nodes are relatively inexpensive and are connected to many others wirelessly. Sensor nodes are also resource constrained as those are equipped with limited memory, limited processing capability as well as limited battery power. Radio is the medium of communication for the sensor nodes. One

© 2005 - 2010 JATIT. All rights reserved.

powerful computer (may be a high end Laptop Computer) acts as the Base Station. The Base Station is considered to be resourceful and reliable. Even it is possible to recharge the battery of the Base Station if it becomes necessary. There is no preexisting infrastructure in the system model. Sensors are deployed and then they form a network including the base station in a self organized manner. It has been assumed that it is possible to know the geographic location of each sensor by itself through a GPS free solution [9].

1.3 Operation

A WSN is a large network of resource-constrained sensor nodes with multiple preset functions, such as sensing and processing, to fulfill different application objectives. The major elements of WSN are the sensor nodes and the base stations. In fact, they can be abstracted as the "sensing cells" and the "brain" of the network, respectively. Usually, sensor nodes are deployed in a designated area by an authority and then, automatically form a network through wireless communications. Sensor nodes of homogeneous or heterogeneous type can be deployed randomly or at pre-determined locations using a deterministic scheme. Sensor nodes are static most of the time, whereas mobile nodes can be deployed according to application requirements. One or several, static or mobile base stations (BSs) are deployed together with the network. Sensor nodes keep monitoring the network area after being deployed. After an event of interest occurs, one of the surrounding sensor nodes can detect it, generate a report, and transmit the report to a BS through multi hop wireless links. Collaboration can be carried out if multiple surrounding nodes detect the same event. In this case, one of them generates a final report after collaborating with the other nodes. The BS can process the report and then forward it through either high-quality wireless or wired links to the external world for further processing. The WSN authority can send commands or queries to a BS, which spreads those commands or queries into the network. Hence, a BS acts as a gateway between the WSN and the external world.

1.4 Data Confidentiality

Data confidentiality is the most important issue in network security. Every network with any security focus will typically address this problem first. In sensor networks, the confidentiality relates to the following :

• A sensor network should not leak sensor readings to its neighbors. Especially in a military application, the data stored in the sensor node may be highly sensitive.

• In many applications nodes communicate highly sensitive data, e.g., key distribution, therefore it is extremely important to build a secure channel in a wireless sensor network.

• Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, thus achieving confidentiality.

1.5 Secure Data Aggregation

As wireless sensor networks continue to grow in size, so does the amount of data that the sensor networks are capable of sensing. However, due to the computational constraints placed on individual sensors, a single sensor is typically responsible for only a small part of the overall data. Because of this, a query of the wireless sensor network is likely to return a great deal of raw data, much of which is not of interest to the individual performing the query. Thus, it is advantageous for the raw data to first be processed so that more meaningful data can be gleaned from the network. This is typically done using a series of aggregators. An aggregator is responsible for collecting the raw data from a subset of nodes and processing/aggregating the raw data from the nodes into more usable data. However, such a technique is particularly vulnerable to attacks as a single node is used to aggregate multiple data. Because of this, secure information aggregation techniques are needed in wireless sensor networks where one or more nodes may be malicious.

2. PROBLEM SPECIFICATION

In order to avoid heavy traffic and conserve energy in a sensor network caused by the transmission of raw data back to the base station from each sensor, data fusion nodes can be deployed in the network. In the data fusion process,

© 2005 - 2010 JATIT. All rights reserved.

a data fusion node receives data from a number of sensors, conducts data fusion, and then sends the result (decision) to the base station. One example of such a system is distributed detection using multi sensor networks as described by Varshney in [3] and further discussed in [4], [5], [6].

The sensor nodes collect data from the environment and make their binary decisions based on some detection rules. Then they send these decisions to the data fusion node. The fusion node decides on the presence or absence of the event in that environment, based on the binary data it received, and then sends this result to the base station. One of the key advantages of this distributed detection and fusion scheme is that it reduces the transmission burden between sensor nodes and the data fusion node. While much effort has gone into the design of fusion algorithms [3], to our knowledge, security and assurance aspects of data fusion systems have not been studied. The current data fusion system puts a great deal of trust on the nodes conducting data fusion. However, if the data fusion node is compromised and becomes malicious, it can send an arbitrary fusion result to the base station. Since the original data are not forwarded to the base station, it is difficult for the base station to verify whether the result is valid1. Moreover, sensors might also be compromised. If a sensor is compromised and becomes malicious, it can send incorrect sensing results to the fusion node. However, because some fusion algorithms can tolerate certain number of malicious sensors, we will assume that the number of compromised sensor nodes is tolerable.

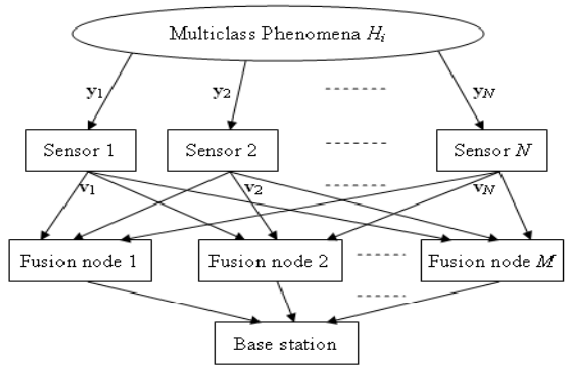

Fig. 1. Structure of a wireless sensor network for distributed detection using N sensors and M fusion nodes

Figure 1 depicts a wireless sensor network for distributed detection with N sensors for collecting environment variation data, and a fusion center for making a final decision of detections. This network architecture is similar to the so-called Sensor with Mobile Access (SENMA) [10], [14] Message Ferry , and Data Mule [8]. At the jth sensor, one observation yj is undertaken for one of phenomena H_i, where i = 1, 2, . , L. If the detection (raw) data are transmitted to the fusion nodes without any processing, then the transmission imposes a very high communication burden. Hence, each sensor must make a local decision based on the raw data before transmission. The decisions, v_j , j = 1, 2, .. . ,N, can be represented with fewer symbols than the raw data. The sensor then transmits the local decision to M fusion nodes using broadcast. The fusion node 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 of the fusion nodes or all of the sensors fail, this detection and fusion scheme can guarantee that the base station can obtain the detection result. However, the accuracy of the result is not certain. Two problems must be solved to ensure that the base station obtain the correct result. First, every fusion node must correctly fuse all of the local decisions, which also implies that all of the fusion results must be the same. Several algorithms have been proposed to deal with this problem [7]. This work assumes that this problem has been solved. The second problem concerns 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 sensor are not sent directly to the base station. Consequently, the result obtained at the base station may be incorrect.

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

© 2005 - 2010 JATIT. All rights reserved.

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[15]. 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 require no extra hardware for data assurance. Here several copies of the fusion data required to sent the base station, so the power consumption for the data transmission is very high. There are two methods are available first one is Witness Based Approach , the second one is Direct Voting Mechanism.

Witness Based Data Assurance Solution was proposed byW. Du, J. Deng, Y. S. Han and P. K. Varshney [16]. Witness based scheme to ensure that the BS accepts only valid data fusion results. To prove the validity of a report, the fusion node is required to provide proofs from several witnesses. A witness is a node that also performs data fusion but does not send its report to the BS.

3 WITNESS BASED DATA FUSION ASSURANCE

Witness nodes to enhance the assurance of data fusion. In order to prove the validity of the fusion result, the fusion node has to provide proofs from several witnesses. A witness is one who also conducts data fusion like a data fusion node, but does not forward its result to the base station; instead, each witness computes the *Message Authentication Code* (*MAC*) of the result (we call the *MAC* a proof), and then provides it to the data fusion node, who must forward the proofs to the base station. If the data fusion node is compromised, and wants to send an invalid fusion result to the base station, it has to forge the proofs on the invalid result. There could be various ways to achieve what we described Let F denote the data fusion node. Assume that we have chosen M witnesses, w_1... w_m and K_1.. K_m and represent the *MAC* keys they share with the base station. above. We assume that the data fusion node and witness nodes share a secret key with the base station. After receiving the data from the sensor node_ each witness i conducts data fusion, and obtains the result S_i it then sends $MAC_i = MAC(S_i, W_i, K_i)$.

3.1 The Witness Based Data Assurance Algorithm

This algorithm to ensure the validity of the data fusion result, here they developed a witness-based mechanism, the base station uses the n-out-of-(m+1) voting strategy[16].

- Let there be m witnesses + 1 data fusion node.
- Each witness w_i share an unique key with the BS, k_i
- After receiving reports from the sensor nodes, each witness performs data fusion and obtains the result r_i.
- It then sends a MAC (Message Authentication Code) to the data fusion node:
- $MACi = MAC(r_i, w_i, k_i)$
- The data fusion node computes its result and sends its MAC key with its witnesses to the BS.
- The BS exercises a voting scheme to determine the validity of the report.
- If the report is corrupted, the BS discards it and polls one of the witness nodes for the correct report.
- The Base Station can employ two voting schemes to determine the validity of the fused report.
- m+1 out of m+1: the result is valid if supported by all the witnesses.
- n out of m+1: (1=<n<=m+1) the result is valid if supported by at least n witness.

4. 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

© 2005 - 2010 JATIT. All rights reserved.

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 is proposed to ensure data fusion assurance.

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 base station can transmit the fusion result of the chosen node to the witness or the witness node is in the communication range of the chosen node and the base station. Therefore, the witness node can obtain the transmitted fusion result from the chosen node through the base station or overhearing. The witness node then can compare the transmitted fusion result with its own fusion result. Finally, the witness node can send its vote (agreement or disagreement) on the transmitted 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.7 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 based on the voting mechanism using a group key.

In this scheme[15], the base station needs to ask the witness node whether it agrees or disagrees with the transmitted fusion result. The witness node then 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 might have to select a witness node that does not agree with the transmitted result as the next chosen node. The detail steps of the scheme are given as follows:

Step 1: The base station chooses a fusion node. Other fusion nodes serve as witness nodes. Define a set of witness nodes that includes all witness nodes and let the nodes in the set be randomly ordered. Denote $M' = M - 1$ as the size of the witness set in the current round.

Step 2: The chosen node transmits its fusion result to the base station.

Step 3: The base station polls the node in the witness set by following the order of the witness nodes. The polling-for-vote8 process does not stop until

- T witness nodes *agree* with the transmitted fusion result (agreeing nodes), where $1 \le T \le M - 1$,
- $M' - T + 1$ witness nodes *disagree* with the transmitted fusion result (disagreeing nodes), or
- all witness nodes have been polled.

Step 4: Represent A as the number of witness nodes that agree with the transmitted fusion result.

- If $A = T$, then the transmitted fusion result passes the verification of the fusion result. Stop the polling.
- If $M' - T - 1 < A < T$, then no reliable fusion result is valid. Stop the polling.
- If $A \le M' - T - 1$, then exclude the A agreeing witness nodes from the witness set. Let the first node that disagrees with the transmitted fusion result be the chosen node to transmit its fusion result.

© 2005 - 2010 JATIT. All rights reserved.

Pros & Cons of Voting 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

5. PROPOSED METHOD

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, witnesses nodes will be silent if there is no compromised nodes. If a compromised node is sending false data, then one or more witnesses 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 .

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.

6. THE SIMULATION AND ANALYSIS

6.1 Hierarchical Fusion Architecture

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

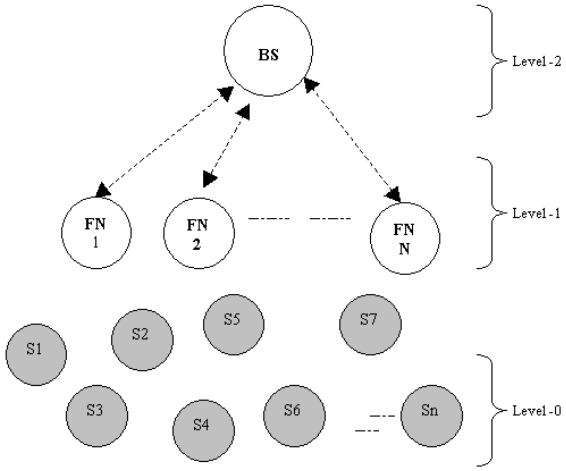

Figure 2 : The Hierarchical Fusion Architecture

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.

The Algorithms going to be implemented on ns2 are :

1. Witness Based Data Fusion Assurance

© 2005 - 2010 JATIT. All rights reserved.

2. Direct Voting Based Fusion Assurance

6.2 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.

6.3 Experimental Setup

We have used the directed diffusion code in NS-2 implemented by USC/ISI[17] and mobility extensions that were implemented by the CMU Monarch project [18]. 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)

6.4 The Simulation Results

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

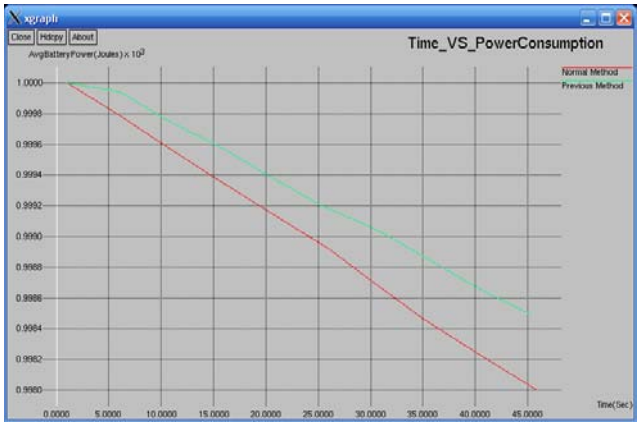

Figure 3 : The Power Consumption

As shown in the above graph, the power consumption during data fusion assurance in the case of previous method (Direct voting) is little bit lower than the normal method (witnessed based).

The following graph shows the MAC Load at fusion nodes and the base station.

© 2005 - 2010 JATIT. All rights reserved.

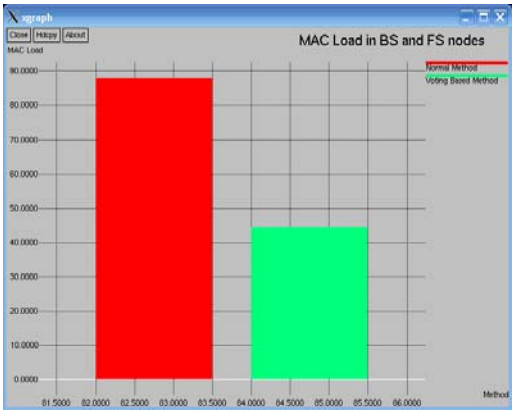

Figure 4 : The MAC Load

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

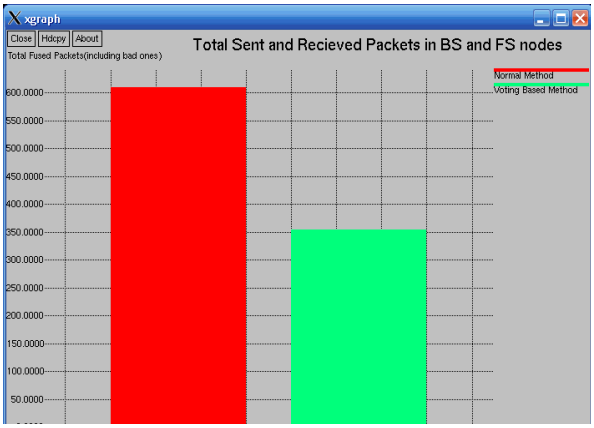

Figure 5: The Overhead in Terms of Received Packets

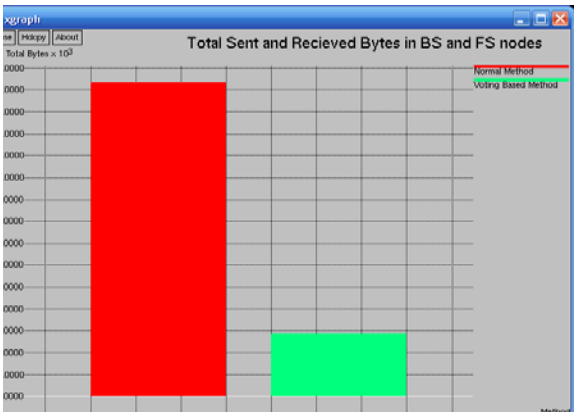

Figure 6 : The Overhead in Terms of Received Bytes

As shown in the above chard the overhead in terms of the received bytes at the fusion node and base station in the voting based method is very low.

7. CONCLUSION

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.Normal MAC based method, 2. Direct Voting Based Method. To ensure the validity of the data fusion result, To reduce energy consumption in our scheme, we have analyzed and computed the minimum length needed for the Message Authentication Code to achieve a pre-defined level of security. Our results show that the number of bits used for MACs does not increase linearly with the number of witnesses.

In this data fusion scheme the base station in the sensor network collects the fusion data and the votes on the data directly from the fusion nodes. This scheme is more reliable with less assurance overhead and delay than the witnessed based approach. Here Polling Scheme is an overhead. Use of a public key is a threat to security. These type of problems to be eliminated in our proposed Data fusion assurance using silent negative voting method .

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].Wei Yuan, Srikanth V.Krishnamurthy, and SatishK. 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.

[3] .P. K. Varshney, *Distributed Detection and Data Fusion*, NewYork,NY: Springer-Verlag, Inc., 1997.

[4]. R. S. Blum, S. A.Kassam, and H.V.Poor, Distributed detection with multiple sensors II. Advanced topics," *Proceedings of*

© 2005 - 2010 JATIT. All rights reserved.

the IEEE, Vol. 85, pp. 64-79, January 1997.

[5] .P. K. Varshney, ed., Special Issue on Data Fusion, *Proceedings of the IEEE*, vol. 85, January 1997.

[6].R. Viswanathan and P. K. Varshney, "Distributed detection with multiple sensors Part I. Fundamentals," *Proceedings of the IEEE*, Vol. 85, pp. 54-63, January 1997.

[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]. L. Tong, Q. Zhao, and S. Adireddy, "Sensor networks with mobile agents," in *Proc. IEEE MILCOM'03*, Boston, MA, Oct. 2003, pp. 688–693.

[10]. 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.

[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.\

[15].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) .

[16].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.

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

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

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

© 2005 - 2010 JATIT. All rights reserved.

AUTHOR PROFILES:

M.Umashankar is a professor at Department of Computer Technology, K.S.Rangasamy college of Technology, Tiruchengode. He is currently a PhD candidate in Computer Application at Anna University, Coimbatore. His research interests include Computer Network, Network Security, Wireless Sensor Networks and Cryptography.

Dr. C. Chandrasekar received his Ph.D. degree from Periyar University, salem. He has been working as a Professor at Dept. of Computer Science, Periyar University, Salem. His research interest includes Wireless networking, Mobile computing, Computer Communication and Networks. He was a Research guide at various universities in India. He has been published more than 50 technical papers at various National/ International Conference and Journals.