International Journal of Wireless & Mobile Networks (IJWMN) Vol. 5, No. 2, April 2013

ENERGY CONSUMPTION IN WIRELESS SENSOR NETWORKS USING DATA FUSION ASSURANCE

S. Kami Makki[1], Matthew Stangl[2] and Niki Pissinou[3]

[1]Computer Science Dept., Lamar University, Beaumont, TX
kami.makki@lamar.edu
[2]Computer Science Dept., Southwestern Oklahoma State University, Oklahoma, OK
stanglm@student.swosu.edu
[3]Computer Science Dept., Florida International University, Miami, FL
pissinou@fiu.edu

ABSTRACT

Data fusion techniques reduce total network traffic in a wireless sensor network, since data fusion can integrate multiple raw data sets into one fused data set. However, the security or assurance of the data requires more processing power and is an important issue. Increasing the security of the fusion data increases factors such as power consumption, and packet overhead. Therefore any data fusion assurance scheme must be power efficient as well as secure. There are currently several methods of data fusion assurance that have been proposed. Therefore, this paper looks at the current data fusion assurance methods and proposes new schemes focused on reducing power consumption. In this paper, several data fusion assurance schemes are also compared to determine which scheme is the most energy efficient.

KEYWORDS

Data aggregation, energy efficiency, information assurance, security, sensor networks

1. INTRODUCTION

1.1. WIRELESS SENSOR NETWORKS

A wireless sensor network (WSN) is a collection of nodes organized into a cooperative network [12]. Each WSN consists of three primary components: sensor nodes, data fusion nodes, and a base station. The sensor nodes are responsible for collecting the locally available sensor data. The sensor nodes are small and inexpensive. Since most nodes are traditionally battery powered, power consumption is an important consideration when setting up a WSN. Once the data has been collected from the sensor nodes, they then transmit that information to a data fusion node.

Due to their limited power and short communication range, the information that the nodes send to the base station is usually put through a data fusion technique before being sent to the base station [1]. This allows for the data to be more accurate and also reduces overhead in the network. The node that performs the data fusion is called the data fusion node.

1.2. DATA FUSION

Multiple sensors combine data and perform data fusion to achieve improved accuracy and inferences when compared to the use of a single sensor node [13]. Data fusion combines diverse data sets into a unified (fused) data set. This allows increasing the accuracy of the transmitted data, increased statistical advantages of the data, and lowering the traffic between the nodes and base station [2].

DOI : 10.5121/ijwmn.2013.5204

1.3. SECURITY ISSUES/CHALLENGES

A data fusion node sends aggregated data to the base station. However, an attack on a data fusion node is more effective than an attack on a regular sensor node. In addition the base station cannot ensure whether the data received is correct, since the base station does not have access to the unfused data from the sensor nodes [2]. In WSNs with multiple levels of transmissions, this problem becomes even more severe. A stealthy attack is an attack that sends false information to the base station. There are two ways to ensure that the data received from a fusion node is correct for a stealthy attack: one is hardware-based and the other is software-based. Hardware-based schemes typically require extra hardware to ensure security, whereas software-based schemes require little or no extra hardware [6]. This paper will focus on software-based schemes that prevent stealthy attacks.

In order to prevent stealthy attacks from succeeding, additional security measures must be taken into consideration. Most security measures that have been proposed are a combination of complex schemes that work to ensure the assurance of the fusion data [2, 1, 4, 6, 9]. WSNs are commonly deployed using batteries making it often difficult to replace or charge the batteries. Therefore, power consumption is a major concern in WSNs. Any data fusion assurance scheme must be power-efficient as well as secure for its implementation for a network.

1.4. POWER CONSUMPTION

There are three types of activities that take up the majority of the power in a sensor node: sensing, computation, and radio operations such as receiving and transmitting. Of these three activities radio operations take up the majority of the power, so an energy efficient scheme should focus on reducing the amount of time spent on receiving and transmitting [3]. Nodes tend to take up more power consumption in receiving than in transmitting. Listening idly to the channel and overhearing packets consume the most of a nodes power.

The remainder of this paper is organized as follows: in section 2 we will look at the previous solutions to a power efficient data-fusion assurance scheme. Section 3 takes a look at two proposed schemes based on the previous schemes. In section 4 the simulation setup is discussed. In section 5 the results from the simulation are analysed. Section 6 will conclude the paper.

2. PREVIOUS SOLUTIONS

2.1. WITNESS BASED APPROACH

In a witness-based approach, nodes act as witnesses to ensure that the correct data is received. Data is first collected from the sensor nodes in its area. Then, instead of forwarding its result to the base station, it instead computes a Message Authentication Code (MAC) of the result. The fusion node then sends the MAC to the base station. Whenever one data fusion node transmits its MAC to the base station, the other nodes act as witnesses. The base station checks with each of the witness nodes to see if they agree with the result of the data fusion node [4].

In a given network there are N nodes with T as a set threshold. The other N-1 nodes act as witness to the transmitted MAC. If the number of nodes who agree with the MAC is at least T, then the base station accepts the result and polls the fusion node for its data. If the number of witnesses who agree with the MAC is less than T, then the base station polls one of the disagreeing nodes and gets the data from it instead.

The witness-based approach has some disadvantages as well. For example, transmitting MACs requires extra power in comparison with other methods since encrypted data tends to be larger than unencrypted data. Each node when compromised could also have its MAC forged, which

then will allow compromised data to be voted in. This could be made more difficult with proper encryption and long enough MACs, but this would increase the power consumption [9]. In addition, if more than T nodes are compromised, the malicious data will get submitted every time. Therefore, this is an issue in every data fusion assurance scheme proposed so far.

2.2. DIRECT VOTING MECHANISM

Direct voting mechanism is based on the witness-based approach. The witness-based method did not assume that the nodes were within contact range of each other and the base station. However, in practice, this tends to be the case. Instead of transmitting a MAC, the chosen node instead sends the fusion data directly to the base station. Each witness node listens to the transmission from the selected fusion node to the base station and calculates a MAC from its own data. The witness node then compares the created MAC with the overheard MAC. Finally each witness node cast its vote (agreement or disagreement) to the base station.

This method is an improvement over the witness-based approach with analytical results up to 40 times better on the overhead [6]. Since direct polling of each witness node introduces extra overhead. Recently, several data fusion assurance schemes have been developed that improve this method by eliminating direct polling, such as the time-slotted and silent negative voting methods.

2.3. TIME-SLOTTED METHOD

Time-slotted voting was designed based on the direct voting mechanism. Each fusion node is assigned a time-slot to broadcast its fusion result. This has the advantage of eliminating the polling process, thus reducing the overhead from polling each node individually. As in the direct-voting mechanism both the base station and the data fusion nodes are assumed to be near enough to each other to overhear each data fusion node [2].

Each node must be synchronized in time with the base station. Once each node is scheduled to transmit, it either transmits its vote, or its fusion result. If the node does not agree with any of the results sent so far, it can send its own data to the base station. The base station accepts the result with at least T votes, where T is a predetermined threshold.

Time-slotted voting contains all of the same advantages as direct-voting as well as additional advantages from eliminating polling [6]. Since each node sends its data at a specified time, this eliminates the overhead created from polling each node allowing the base station to consume less power. Time-slotted voting also works better than the previous method in multi-hop networks since the base station can act as a fusion node in larger networks. This method is also simpler to implement than direct voting since each node has the same task [9].

2.4. SILENT NEGATIVE VOTING

The silent negative voting method is based on the direct voting mechanism. The nodes are assumed to be able to overhear the transmissions between each other and the base station. The base station first randomly chooses a node to transmit its data. The node then creates an encrypted MAC from its fusion data using its own private key. The node then sends the MAC to the base station. Once the base station receives the MAC it decrypts it. The base station then reencrypts the MAC with a public key and broadcasts it out to the other nodes. Once each node receives the newly encrypted MAC they compare it with a MAC created from the locally available fusion data. If the results agree with each other, then the node is silent. However if the nodes MACs disagree, then the fusion node will send a negative vote, along with a newly encrypted MAC to the base station. If the negative votes surpass a threshold T then the base

station requests one of the disagreeing nodes for its fusion data. If T is under the acceptable level than the base station polls the original fusion node for its fusion data [1].

Silent negative voting eliminates several problems that existed with the direct voting mechanism. Since a node only needs to broadcast a vote if it has been compromised and hence power consumption is reduced. Also, since it is assumed that the probability of a compromised node is less than that of a malicious node, silent negative voting consumes less power overall than direct voting. When compared with time-slotted voting, the round time is less in silent negative voting since it eliminates the scheduled rounds, and instead sends out the data after it receives it from the original data fusion node.

3. THE PROPOSED METHODS

Since most of the power consumption in data fusion nodes results from listening idly to the channel and overhearing packets, a power efficient data fusion assurance scheme should focus on reducing the amount of time that a node spends receiving. The receiving power of a node can be reduced primarily in one of two ways: either reducing the time of a voting round, or putting a node to sleep [7]. This paper takes the silent negative voting and time-slotted methods and implements solutions based on reducing the time of a voting round, as well as putting the nodes to sleep.

In the previous methods, if more than T nodes are compromised, the malicious data will get submitted every time. In addition to focusing on conserving power, additional data security can be gained by counting the number of compromised nodes. Once the number of compromised nodes has reached a certain threshold, then the data network is considered corrupted, and the base station won't accept any more fusion data from it.

3.1. SILENT NEGATIVE VOTING METHOD USING SLEEP/WAKEUP SCHEDULE

This method is based on silent negative voting with a focus on reducing the power consumption of the nodes. It works based on the same principles as the silent negative voting method with a few differences. The base station and the data fusion nodes are synchronized in time with each other. Normally in silent negative voting, the voting round begins with choosing a specific node and polling it for its MAC. Instead, in this method, the base station asks the node directly for its fusion data. Once the node sends its data, it goes to sleep, allowing it to conserve energy. The base station calculates a MAC from the fusion data it receives and then transmits the MAC to the other nodes [9].

Each fusion node compares the received MAC to a MAC created from the locally available data. If the calculated MAC agrees with the base station's MAC, then the node falls asleep. If the two MACs disagree, then the node sends its own encrypted MAC to the base station, and then falls asleep. Since both the base station and the fusion nodes are synchronized in time, the nodes wakeup once the voting round is over. If the base station's original MAC did not have enough votes to pass the threshold T, then the base station polls one of the dissenting nodes for its fusion data instead.

When compared to regular silent negative voting, this method has the advantages of reduced data latency and reduced power consumption. Since the time for each voting round is reduced, energy is conserved because each node listens for less time than before. The security advantages of this method are the same as the silent negative voting method. The data fusion nodes do not always need to be listening to the receiving channel since there are less data packets. The data fusion nodes can therefore be put to sleep to conserve energy. This leads to a reduction in energy consumption.

3.2. TIME-SLOTTED VOTING METHOD USING SLEEP/WAKEUP SCHEDULE

This method is based on the time-slotted voting method. It runs similar to the time-slotted voting method with a few key differences. Once a node has reached its appointed time-slot, it either votes or transmits its fusion data. However once the node has transmitted its result it then goes to sleep until the end of the round.

The base station will pass the accepted result if it has at least a threshold T number of votes. However once the data reaches T number of votes it sends a message to the fusion nodes ending the round and waking up the nodes that are asleep, thus decreasing the round time. If there were not at least T votes at the end of the round, then the base station accepts one of the results from the dissenting nodes.

This method has several advantages over regular time-slotted voting. Since the nodes are put to sleep after they transmit their information, they consume less power than the normal time-slotted voting. Additionally, since each round ends at either the allotted time, or once T votes have been reached, the voting time will be reduced compared to normal time-slotted voting, thus reducing the data latency.

4. SIMULATION

The simulation was conducted using the OMNeT++ simulation environment with the MIXIM framework [15, 14]. Additional functionality for controlling radios in the wireless sensors was implemented using an extension of the MIXIM framework [5].The data fusion nodes correctly fuses the data. The simulation is focused on deliverance of fused data to the base station. Once each packet has been sent, it is assumed to arrive at its destination error free.

Table 1: Message parameters

Parameters	Values
MAC(Message Authentication Code) packet	64 bytes
Application layer header	512 bits
Network header	32 bits
MAC(Medium Access Control) layer header	24 bits
Physical layer header	48 bits

The fusion data parameters were taken from either the standards provided by OMNeT++ and MIXIM, or from the silent negative voting method [1]. These parameters are shown in Table 1.

4.1. SIMULATION SETUP

Four different wireless sensors were used in the simulation. Each of the wireless sensors parameters are taken from the CSMA-CA MIXIM framework or the wireless sensors datasheet [11]. The four different wireless sensors used are: TI CC1100, Mica2, MicaZ, and TelosB. The energy parameters used in the simulations are shown in Table 2.

Three different simulations were conducted. Each simulation was conducted with one base station and 5, 10, or 50 data fusion nodes in the WSN. To simulate a stealthy attack it is assumed that 1 out of every 5 nodes will be compromised. Therefore, each node has a 20% chance of being compromised. The threshold T that a data fusion result needed to pass for the

simulations was assumed to be 40%. The methods implemented in the simulations are: silent negative voting, time-slotted voting method using sleep/wakeup scheduling, and silent negative voting method using sleep/wakeup scheduling. The experiment was conducted for 10,000 simulation seconds for each network size.

Table 2: Node parameters

Parameters	rx Current	tx Current	sleep current
TelosB	21.8 mA	19.5 mA	2.6 µA
Mica2	15.1 mA	25.4 mA	20 µA
MicaZ	23.3 mA	21.0 mA	20 µA
TI CC1100	16.4 mA	17.0 mA	20 µA

5. SIMULATION RESULTS

5.1. FIVE NODES NETWORK

Figures [1-4] show the average power consumption for each method implemented. Each graph shows the power consumption of a different wireless sensor, as well as the power consumption for both the nodes and the base station. These results are from a 5 node network. As these graphs show, while total power consumption varies depending on the type of wireless sensor, uniform results are received no matter which wireless sensor is compared.

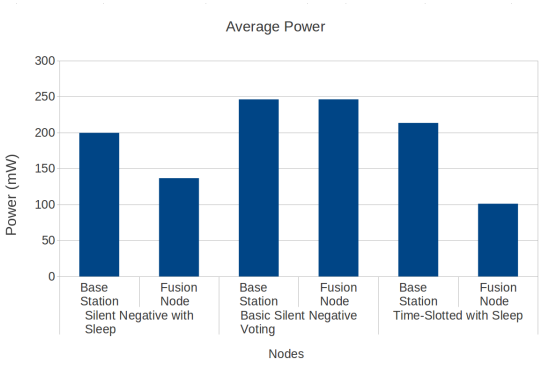

Figure 1: Average power consumption for TI CC1100

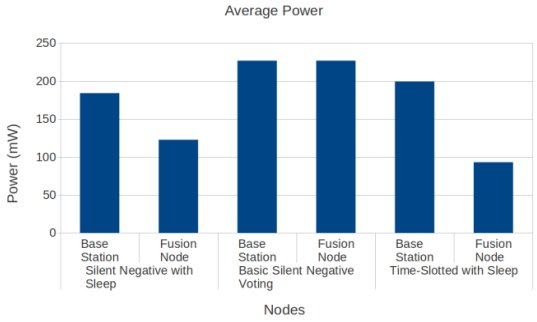

Figure 2: Average power consumption for Mica2

As shown in figures [1-4], the time-slotted method with sleep/wakeup scheduling is the most power efficient method when comparing the power consumption of the nodes, with the silent negative method with sleep/wakeup scheduling slightly less power efficient.

However when comparing the power consumption of the base station in the experiment, the most power efficient method is the silent-negative method with sleep/wakeup scheduling. The other two methods are less power efficient overall when comparing the power consumption of the base stations.

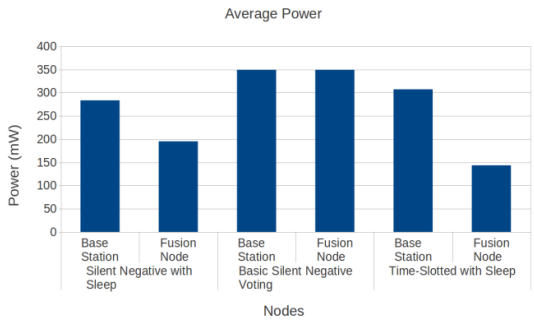

Figure 3: Average power consumption for MicaZ

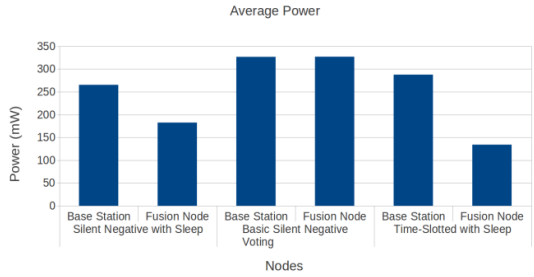

Figure 4: Average power consumption for TelosB

Figure 5 shows the average times for each voting round. Short voting round times are important since a short voting round means reduced data latency. The silent negative method with sleep/wakeup scheduling has the shortest average voting times. The time-slotted method with sleep/wakeup scheduling has slightly longer average voting round times, and the silent negative method has the longest average voting round time.

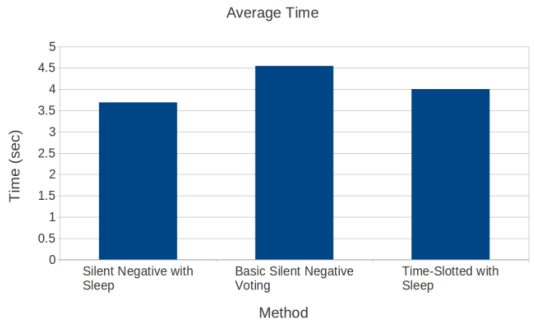

Figure 5: Average time of one voting round

5.2. TEN NODES NETWORK

Figures [6-9] show the average power for the simulations conducted in a 10 node WSN. Each graph shows the average power consumption of a different wireless sensor. The most power efficient method, when analysing both the node and base station power consumption, is the silent negative method with sleep/wakeup scheduling. The node power consumption of the time-slotted method with sleep/wakeup scheduling is less than that of the silent negative method; however, in the simulation, the base station consumes significantly more power.

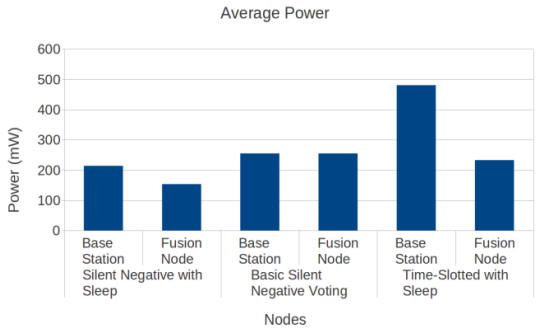

Figure 6: Average power consumption for TI CC1100

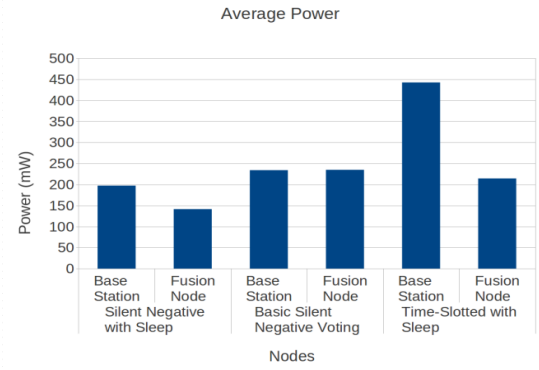

Figure 7: Average power consumption for Mica2

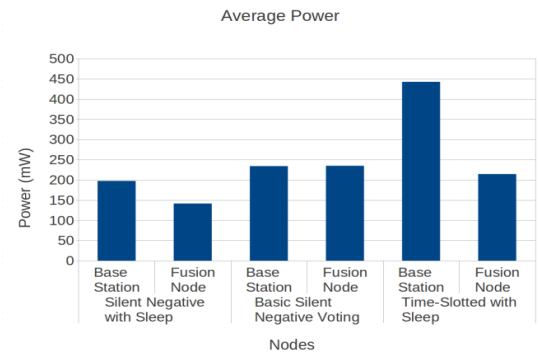

Figure 8: Average power consumption for MicaZ

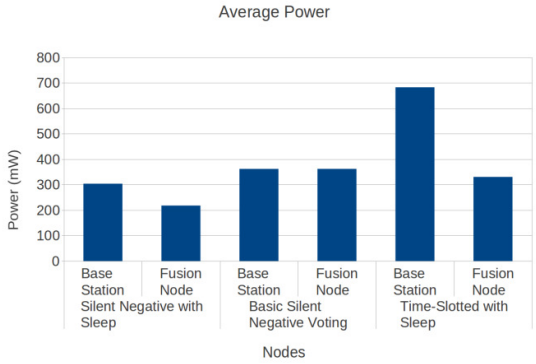

Figure 9: Average power consumption for TelosB

Figure 10 shows the average time per voting round. This figure shows that the silent negative method with sleep/wakeup scheduling has the shortest voting rounds. Figure 10 also shows that the time-slotted method with sleep/wakeup scheduling voting round time increases much quicker than other two methods.

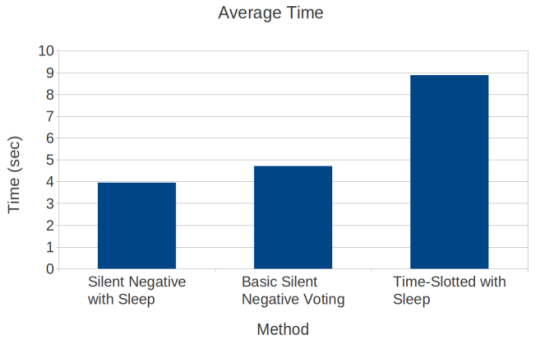

Figure 10: Average time of one voting round

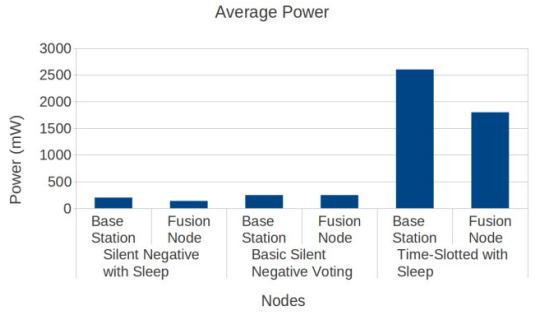

Figure 11: Average power consumption for TI CC1100

5.3. FIFTY NODES NETWORK

Figures [11-14] show the average power for the simulations ran in a 50 node WSN. Each graph shows the average power consumption of a different wireless sensor. The method which consumes the least amount of power is the silent negative method with sleep/wakeup scheduling. The next most power efficient method is the silent negative method. The time-slotted method with sleep/wakeup scheduling consumes much more power when compared to the other two methods.

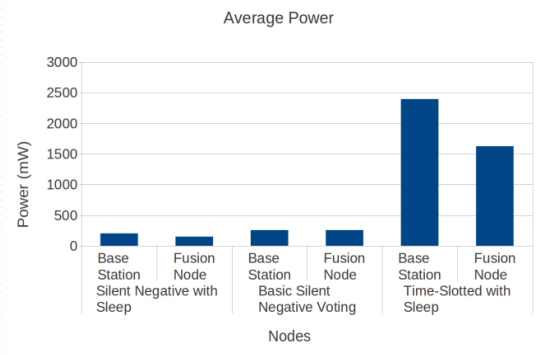

Figure 12: Average power consumption for Mica2

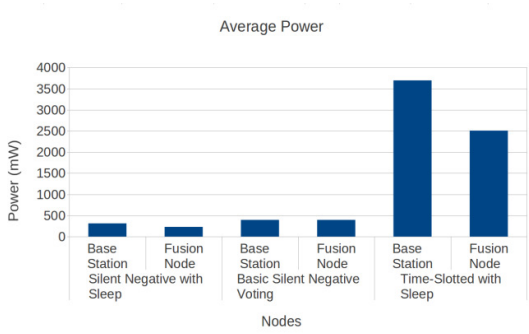

Figure 13: Average power consumption for MicaZ

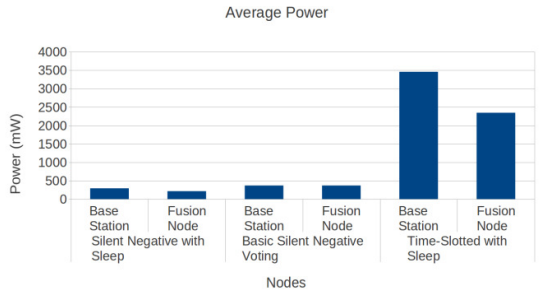

Figure 14: Average power consumption for TelosB

Figure 15 shows the average time per voting round in a 50 node WSN. This figure shows that the silent negative method with sleep/wakeup scheduling has the shortest rounds. The alternate time-slotted method rounds are by far the longest. Since the time-slotted voting method with sleep/wakeup scheduling is based on each node voting at a set time, the average voting round times are going to get consistently longer as the number of nodes increases. Both silent negative voting methods average voting round times increase as the network size increases, however the rate of increase is much slower. The reason why silent negative voting based schemes average voting round times are shorter is because each node does not have a specific time to vote; instead the witness nodes are polled all together.

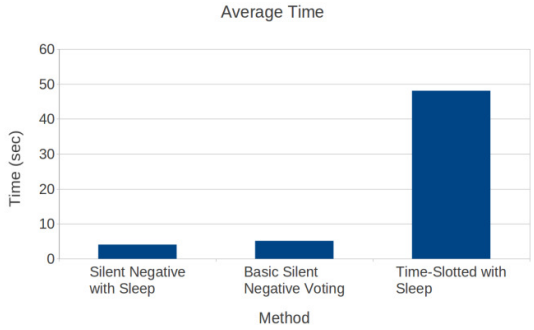

Figure 15: Average time of one voting round

6. CONCLUSION

As the simulations show, the silent negative method with sleep/wakeup scheduling is a more power efficient method than regular silent negative voting. In every simulation the silent negative method with sleep/wakeup scheduling has the shortest voting time, meaning that it had the least data latency among all of the methods tested. However, in the 5 node WSN its nodes were not the most power efficient.

The results of simulations for the network of 5 nodes shows that the time-slotted method with sleep/wakeup scheduling performed very well in both the average voting round time, and the average power consumed by the node. However, once the size of the network increased both the average voting round time and average power per round increased drastically. Therefore, the time-slotted method with sleep/wakeup scheduling is more suitable for a small network environment.

In summary, the most power efficient data fusion assurance scheme is the silent negative method with sleep/wakeup scheduling. This method performs consistently better than the other methods when network size is taken into consideration. Even though the time-slotted method with sleep/wakeup scheduling performs better on smaller networks, the silent negative method with sleep/wakeup scheduling is superior since it is both scalable in size, and in small networks it also is power efficient.

REFERENCES

[1] C. Chandrasekar and M. Umashankar, "Power Efficient Data Fusion Assurance Scheme for Sensor Network using Silent Negative Voting," International Journal of Computer Applications, Vol. 1, No. 4, 2010.

[2] H.-T. Pai, J. Deng, and Y. S. Han, "Time-Slotted Voting Mechanism for Fusion Data Assurance in Wireless Sensor Networks under Stealthy Attacks," Computer Communications, Vol. 33, No. 13, pp.1524-1530, 2010.

[3] A. Roy and N. Sarma, "Energy Saving in MAC Layer of Wireless Sensor Networks: a Survey", National Workshop in Design and Analysis of Algorithm (NWDAA), Tezpur University, India, 2010.

[4] 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, Vol. 3, pp. 1435-1439, San Francisco, CA, 2003.

[5] O. Helgason and S. T. Kouyoumdjieva, "Enabling Multiple Controllable Radios in OMNeT++ nodes", in Proceedings of ICST Conference on Simulation Tools and Techniques (SIMUTools'11), OMNeT++ workshop, Barcelona Spain, March 2011.[6] Hung-Ta Pai

and Yunghsiang S. Han, "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), July 2006.

[7] Fatma Bouabdallah, Nizar Bouabdallah, Raouf Boutaba. "On Balancing Energy Consumption in Wireless Sensor Networks", IEEE Transactions on Vehicular Technology, Vol. 58, No. 6, pp. 2909-2924, 2009.

[8] Guoliang Xing, Rui Tan, Benyuan Liu, Jianping Wang, Xiaohua Jia, Chih-Wei Yi, "Data Fusion Improves the Coverage of Wireless Sensor Networks", ACM MOBICOM 2009, pp. 157-168.

[9] Ramon Sandoval, S. Kami Makki, and Bo Sun, "Utilizing Silent Negative Voting and Sleep/Wakeup Method for Power Efficient Data Fusion", IEEE Computing, Networking and Communications (ICNC), pp. 1000-1004, 2012

[10] “Telos (Rev B.): PRELIMINARY Datasheet (12/5/2004)", Moteiv Corporation

[11] Joseph Polastre, Robert Szewczyk, and David Culler, "Telos: Enabling Ultra-Low Power Wireless Research", Information Processing in Sensor Networks, pp. 364-369, April 2006.

[12] J. A. Stankovic, "Wireless Sensor Networks", Computer, Vol. 41, Issue 10, pp. 92-95, Oct. 2008

[13] David L. Hall, "An Introduction to Multisensor Data Fusion", Proceedings of the IEEE, Vol. 85, Issue 1, pp. 6-23, Jan. 1997.

[14] MIXIM, http://mixim.sourceforge.net/

[15] OMNeT++, http://www.omnetpp.org/