A GENERIC TECHNIQUE FOR INTERCONNECTION BETWEEN WSN AND IP NETWORK

Karim A. Emara* Mohammad Abdeen* Mohammad Hashem*
*Ain Shams University, Faculty of Computers and Information Sciences, Cairo, Egypt
kemara@eun.eg mabdeen@asunet.shams.edu.eg mhashem100@yahoo.com

Abstract: *Many applications of wireless sensor network (WSN) require interconnection with IP networks whether for monitoring or control. Such interconnection is not obvious because of the variety of sensor networks architectures and non-standardized protocols. There are many techniques that handle this problem. In this paper, we enhance and evaluate a previously proposed framework by the authors which provides a transparent interconnection between WSN and IP network. This framework is generic in the sense that it can work for both address-centric and data-centric WSNs. Unlike other popular approaches, our approach does not require modifications in the protocol stacks of both networks. In this work, we implemented this framework to evaluate its performance and efficiency and compare it with other approaches.*

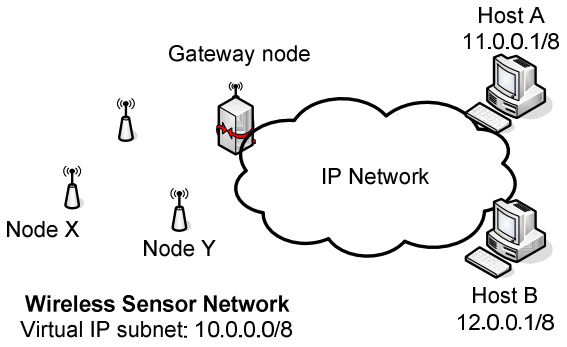
Keywords: *Wireless sensor network, Gateway, IP network interconnection*

1. Introduction

Wireless sensor network (WSN) is an application-centric network, whose main purpose is to obtain physical information from the environment where it is deployed [1]. These networks have several restrictions, e.g., limited energy supply, limited computing power, and limited bandwidth of the wireless links connecting sensor nodes [3]. This results in developing customized proprietary protocols to fit with these restrictions. Such protocols are not compatible with standard TCP/IP networks and Internet.
On the other hand, it is usually desirable to interconnect WSN with the enterprise network to extend its service to remote applications. Therefore, many researchers investigated this interconnection problem. Mainly, there are two interconnection approaches; the gateway-based approach and the TCP/IP overlay [7]. A brief survey about these approaches is discussed in section 4. More details about them can be found in [1], [6] and [7].
The authors in [2] proposed a framework for transparent interconnection between sensor networks and IP network. This framework supports both address-centric and data-centric WSNs. It uses a low-level gateway node to translate traffic from one network to the other. Thus, it allows freely choosing WSN communication protocols that are suitable for the sensor network application. Furthermore, it depends on a simple translation operation and does not require modification to be made in protocols running in either network. Therefore, it can be used with different applications with no need to modify the gateway logic. Moreover, this framework provides transparent communication between both networks. In other words, IP hosts communicate with sensor nodes using virtual IP addresses and sensor nodes communicate with IP hosts using virtual sensor node IDs. In this paper, this framework is enhanced and implemented to evaluate its performance and efficiency.
The rest of the paper is organized as follows. In section 2, the operations of the interconnection technique are discussed. The implementation details and experimental results are shown in section 3. Finally, in section 4, the evaluated technique is compared with the related work.

2. The Interconnection Technique

The interconnection technique proposed in [2] is a gateway-based where the gateway node is connected to both networks and has their protocol stacks, as shown in Figure 1. However, a filter layer is embedded before network layer to filter the traffic forwarded to virtual addresses. If a packet is targeting a virtual IP address or a virtual ID, the filter layer forwards it directly to the gateway application. Otherwise, the packet goes normally in its protocol stack. The gateway application performs the virtual address assignment and packet translation components as specified in [2].
The proposed technique allows direct accessing to individual sensor nodes and network-based querying for data-centric networks. The direct access is usually used in reprogramming or configuration of specific nodes. While data query is often targeting multiple unknown nodes and this is a typical communication paradigm in most sensor networks. Next, we show the detailed design for each case.



Sensor Node
Application
T
N
M

Gateway Node	
Gateway App	
T	UDP
N	IP
Filter Layer	
M	MAC

IP Host
Application
UDP
IP
MAC

Figure 1. Interconnection between WSN and IP network using a gateway

2.1 Direct Access to Sensor Nodes

When sensor nodes have unique IDs over the network, the gateway node assigns a virtual IP address for each sensor node. This address assignment process happens when the gateway receives a packet from this node or when an IP host requests to communicate with it. In the later case, the gateway just assigns a free IP address from the virtual address space with no need to check the existing of this node.
The gateway node performs the same operation with sensor nodes when they want to communicate with IP hosts. It assigns virtual IDs to IP hosts when it receives packets from them. However, it is assumed that the sensor node does not initiate the connection but it replies to a previous packet received from an IP host. This is a typical request flow pattern initiated by a sink (i.e. an IP host) to a source (i.e. a sensor node) while data flows in the reverse direction as a response. Moreover, the virtual ID assignment is controlled by a leased time to ensure scalability. The leased time is a design parameter determined by a tradeoff between the size of the virtual address space and the stability of the interconnection between both networks.
The virtual IP addresses and virtual IDs are not assigned physically in nodes or hosts. However, they are stored in mapping tables maintained by the gateway such as those shown in Figure 2. When hosts and nodes communicate together, they use virtual addresses as destination in their packet format; The IP

host puts the virtual IP address of sensor node in destination field of IP header. Also, the sensor node puts the virtual ID of IP host in the destination field of the routing protocol header. The traffic targeting virtual addresses, must reach to the gateway node to be translated. For the IP network, the router behind the gateway should be configured to forward such packets to the gateway. For the sensor network, the routing protocol used in the network is responsible to reach such packets to gateway. This is done normally as the packets of virtual IDs are originating from the gateway node and the replied traffic returns to it.

Host IP	Virtual ID
11.0.0.1	Host A
12.0.0.1	Host B

Sensor ID	Virtual IP
Node X	10.0.0.1
Node Y	10.0.0.2

Figure 2. Virtual Addresses Mapping Tables for network in Figure 1

When the gateway node receives a packet targeting a virtual address, it is filtered and forwarded to the gateway application. The gateway application translates the packet addresses to the corresponding ones using mapping tables. It does not change or translate the payload of the packet but it copies the payload to the new packet. It is assumed that the applications running in both networks are the same. This technique suggests UDP as a transport protocol in IP network because of the suitability with delayed high error rate sensor networks. However, it can operate theoretically with TCP too, but more research is required in this point to handle issues such as how to filter non-data packets and extending the reliable transmission to the sensor nodes.

2.2 Data Centric Sensor Networks

Sensor networks are usually data-centric networks in which the data is requested based on certain attributes [3] and the sensor nodes lack fabrication-time identifiers [4]. Therefore, it is not compatible with address-centric IP network. The interconnection technique is modified in this case to address *data queries* rather than individual nodes. When IP host wants to request a query from sensor network, it sends the query to the gateway. The gateway caches the query, assigns it a virtual IP address and replies the host by this virtual address. It also keeps the hosts addresses in a mapping table as shown Figure 3. It assigns a lease time for that virtual address whether till the query expiry time or for a preconfigured duration. It then broadcasts the query to sensor network according to its routing protocol. When data is disseminated to the gateway, it forwards data to the cached IP hosts. The source address of such data messages is the virtual IP address of that query.

Attribute-based Query	Virtual IP	Registered Hosts
type=…,interval=…, rect={…}, temperature = …	10.0.0.1	11.0.0.1, 12.0.0.1, …
type=…,rect={…}, humidity = …	10.0.0.2	11.0.0.1, …

Figure 3. The mapping table of a data-centric network

The gateway acts as a sink in such case but receives its queries externally from IP network, see Figure 4. Therefore, it has the application of the sensor network to handle received queries accordingly. When another IP host wants to register for a query or change values of its attributes, it can send the query toward the virtual IP address. When the gateway receives a packet targeting a virtual address, the payload of the packet is forwarded directly to the application and the source IP address (i.e. the address of IP host) is added to the mapping Table 1n the registered hosts.

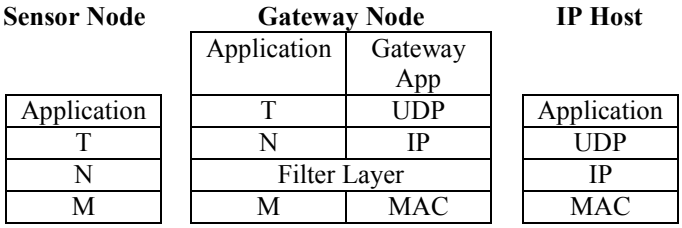


Figure 4. Interconnection technique in data-centric networks

3. Experiments and Results

This technique is implemented on OMNeT++ simulator. The OMNeT++ simulator is an extensible, modular, component-based C++ simulation library and framework [10]. It is a general purpose simulation engine but there are extensions for simulating TCP/IP networks such as INET framework [12] and for simulating sensor networks such as Castalia [13]. As the interconnection technique requires both WSN and IP network, the INET framework and Castalia were integrated in a single framework to allow using features and protocols of both.

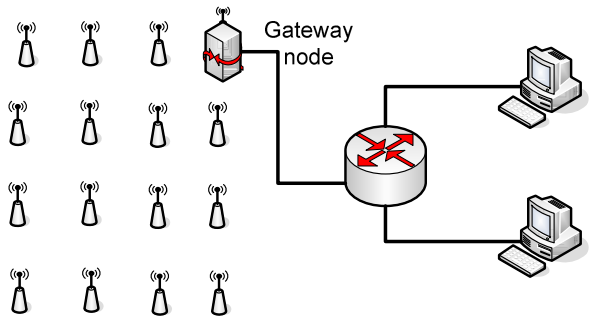


Figure 5. Simulation Environment

The experiments try to show the overhead of the interconnection technique. It compares between results when the experiment runs totally within the sensor network and when it runs over the integrated networks. The simulation environment is similar to that shown in Figure 5. Sensor network uses a *realistic* wireless channel specified in Castalia. It uses CSMA/CA as the data link protocol. Number of nodes ranges from 10 to 290 nodes deployed in a grid field with constant density. For the IP network, hosts ranges from 2 to 5 hosts which use a UDP application to communicate with the gateway node. The router is configured to forward traffic targeting virtual IP addresses to the gateway node.

For the direct accessing mode, results are measured by average end-to-end delay, total throughput, and packet delivery ratio. Average end-to-end delay is the average time it takes a data packet to reach the destination. Throughput is the total number of delivered data packets divided by the total duration of simulation time. Packet delivery ratio is calculated by dividing the number of packets received by the destination through the number of packets originated by the application layer of the source.
The first experiment is to query two specific nodes with different data rates range from 10 to 150 requests per second. As shown in Figure 6, the average end-to-end delay is shown for both runs. We can see that the delay of IP-WSN case is greater than the local WSN case by a nearly constant value. This difference includes the IP network delay plus the integration technique latency to process and forward incoming packets. It is clear that the overhead of the integration technique is almost constant even with high data rates. In Figure 7, the packet loss ratio is shown for both runs. Initially, the packet loss ratio is

almost the same for both runs in common data rates (less than 70 request/second). In 70 requests rate, the packet loss of local WSN traffic is greater than that of IP-WSN traffic. This increase does not indicate that the integration technique enhances the packets delivery, but it only results from random failures in some packets in the first run. In fact, there were only three lost requests in local WSN traffic over those happened in the IP-WSN traffic which is a small difference in packet loss. In higher request rates, packet loss ratio of IP-WSN traffic becomes greater than that of local WSN traffic. The difference in packet loss is in range of 1% - 2% which is acceptable specially in WSN communication. However, it indicates that the packet loss is increased in the integrated network. This may be resultant from the single gateway node that cannot afford to handle all requests which indicates to a bottleneck problem.

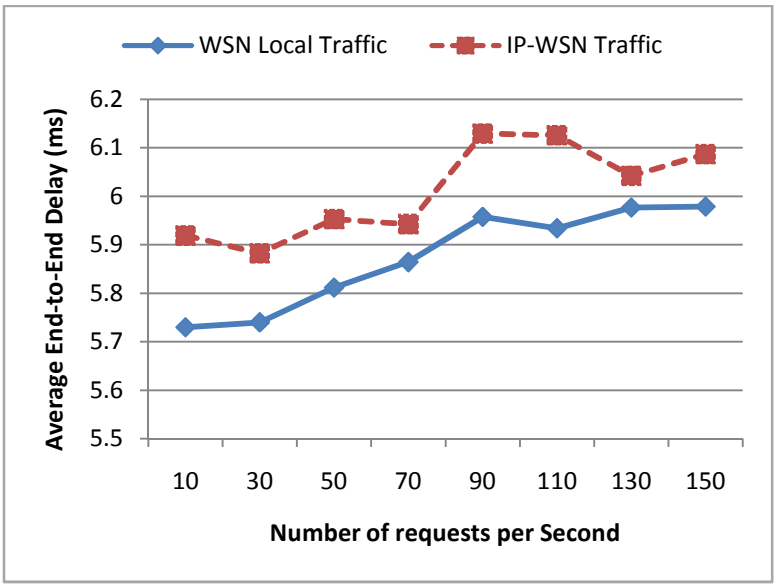


Figure 6. Average End-to-End Delay

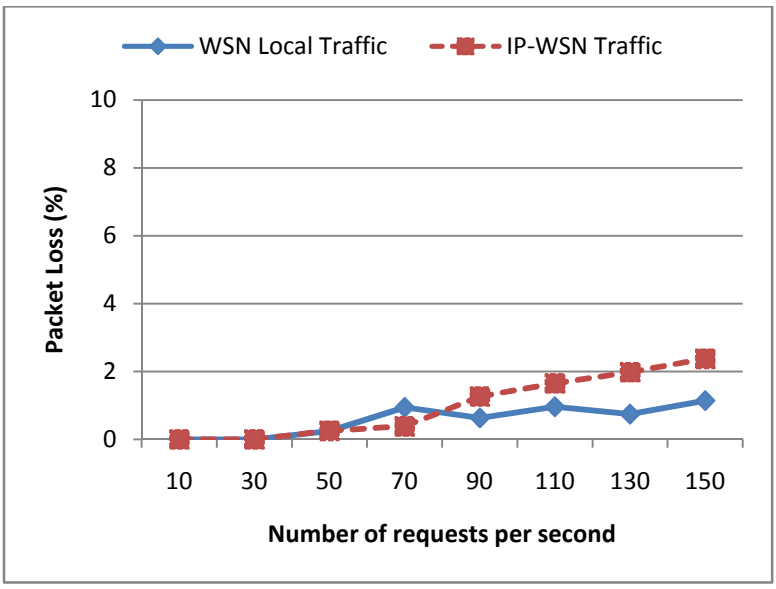


Figure 7: Packet loss ratio versus request rate

In Figure 8, the throughput is almost not affected except in high data rates. This indicates the bottleneck problem of the gateway.

The second experiment tests the effect of the number of requesting IP hosts on the integration technique performance. In this experiment, a set of nodes are configured to query random sensor nodes with constant data rate of 50 requests per second. This experiment is run twice too; the first run operates in sensor network only where sinks requests samples from other sensor nodes. The second run works across IP and sensor networks. In this case, a number of IP hosts are configured to query random sensor nodes in WSN. The number of hosts/nodes range from 1 to 5.

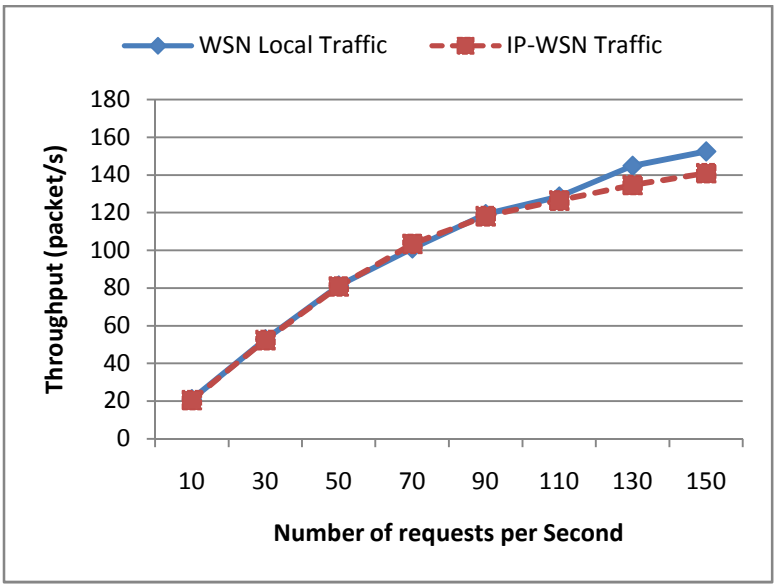


Figure 8. Throughput

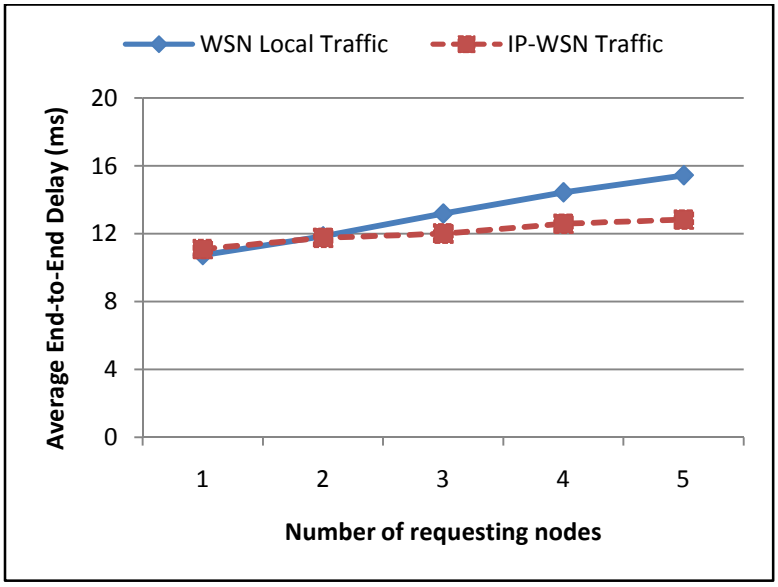


Figure 9. Packet Delivery Ratio

In Figure 9, the average delay of both runs is shown. It shows that the delay of local WSN traffic is higher than that in IP-WSN traffic. One possible explanation for this which is that sinks in the first run request samples from multiple nodes simultaneously which makes the medium busy with their packets. As nodes use CSMA/CA MAC protocol, they wait every time they send a packet which delays transmitting the packet. On the other hand, in IP-WSN case, the gateway is the only node that requests samples on behalf of IP hosts. This makes the medium relatively free as compared to the first run and so allows the gateway to send its packets faster. This network congestion becomes higher with the increasing number of sending nodes, which increases the average delay but it increases more in local WSN traffic for the reason we mentioned.

The packet loss ratio of both runs is plotted in Figure 10. Again, the packet loss of local WSN traffic is surprisingly higher than that of IP-WSN traffic. It can be explained by the interference happens among nodes when sinks send their requests in local WSN case. Such interference increases the failure of packets reception at sensor nodes. On the other hand, in IP-WSN traffic, the gateway is the only requesting node in WSN which makes the interference much less than that in the first run. This increases the chances for the packets to reach their destination and so decreases the packet loss ratio in IP-WSN than that in local WSN traffic case.

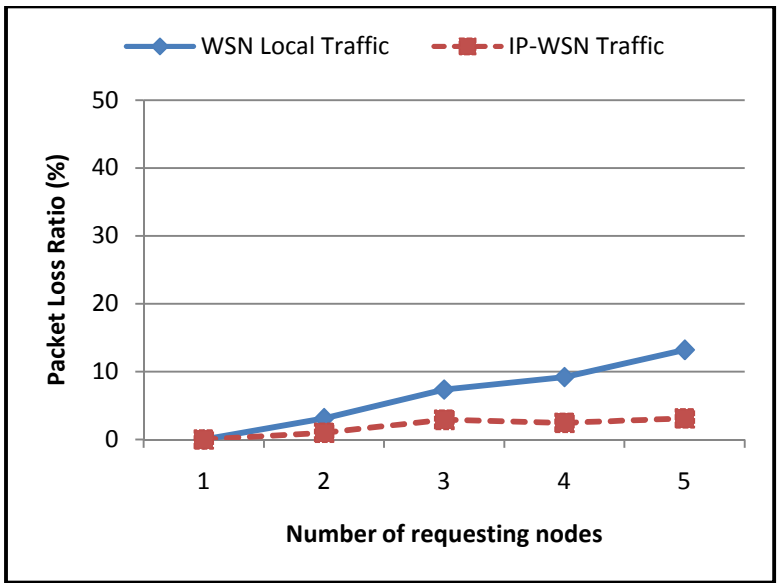


Figure 10: Packet loss ratio versus number of nodes - direct access to sensor nodes

For the data-centric mode, the Directed Diffusion [5] is implemented as it is not included in Castalia. Directed Diffusion is a popular data aggregation paradigm for WSNs. In directed diffusion, sensors measure events and create gradients of information in their respective neighborhoods. The base station requests data by broadcasting interests. Interest diffuses through the network hop-by-hop, and is broadcasted by each node to its neighbors. As the interest is propagated throughout the network, *gradients* are setup to draw data satisfying the query towards the requesting node [3]. The experimental results are measured by average delay and distinct event delivery ratio. Average delay measures the average one-way latency observed between transmitting an event from the source and receiving it at the sink. The distinct-event delivery ratio is the ratio of the number of *distinct* events received to the number originally sent. These metrics were used in [5] to evaluate the performance of directed diffusion.

The first experiment of directed diffusion tests the effect of sensor network size on the performance of the gateway in data-centric mode. The gird size of sensor network ranges from 7x7 to 17x17 nodes (i.e. 49 – 289 nodes). Again, this experiment is run twice. In the first run, a sensor node (i.e. sink) populates an interest matching the farthest node in the network with a refreshment rate one second. The matching node replies by their data messages with interval of 50 milliseconds. The interest expires at the end of the simulation. In the second run, an IP host is configured to query WSN with the same interest used in the first run. Also, the sink node acts as a gateway node in this run to ensure the same network configuration and settings of both runs. We tried initially to use 20, 10 and 5 interests to be used instead of a single interest. However, each interest generates a large number of packets in the network according to its recursive broadcasting to neighbors with periodical refreshment which causes network congestion. For example, when using 5 simultaneous interests in the sink, no interest delivery achieved in even medium-sized networks (i.e. a 13x13 network). Therefore, we chose to use a single interest in this experiment to test large network sizes.

Regarding the average delay, results are compared together as shown in Figure 11. It can be inferred that the integration technique does not add delay to the network even in large network sizes. This result is expected according to transmitting a single interest. However, the delay of integration technique will not be comparable with sensor network delay even with multiple interests. This is according to the limited processing made on each interest in the gateway specially if compared with the delay of sensor network.

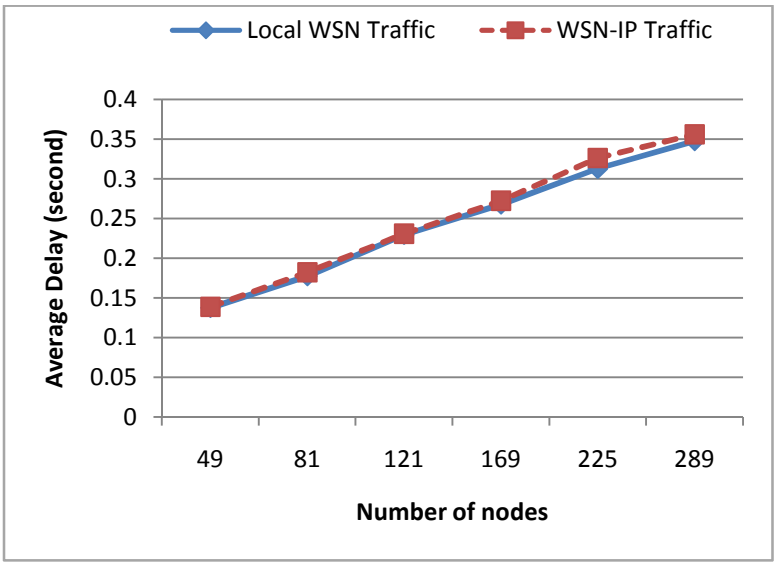


Figure 11. Average Delay with Directed Diffusion

The distinct delivery ratio of both runs is presented in Figure 12. The ratio of both runs is almost the same in different network sizes. At the largest network size, the delivery ratio is decreased slightly in the IP-WSN run but it does not indicate it is caused by the gateway because it happens accidently in a single sample. Also, it is expected that the difference between delivery ratios of both runs will take a similar pattern even with more interests. This is inferred by the fact that this single interest is already sent many times during the interest refreshment made by the requesting node. Also, the matching nodes (i.e. sources) reply by their data messages repeatedly every data interval. Therefore, the given delivery ratio is based on multiple requests and replies which simulate multiple interests but with less data reporting interval and refreshment rate.

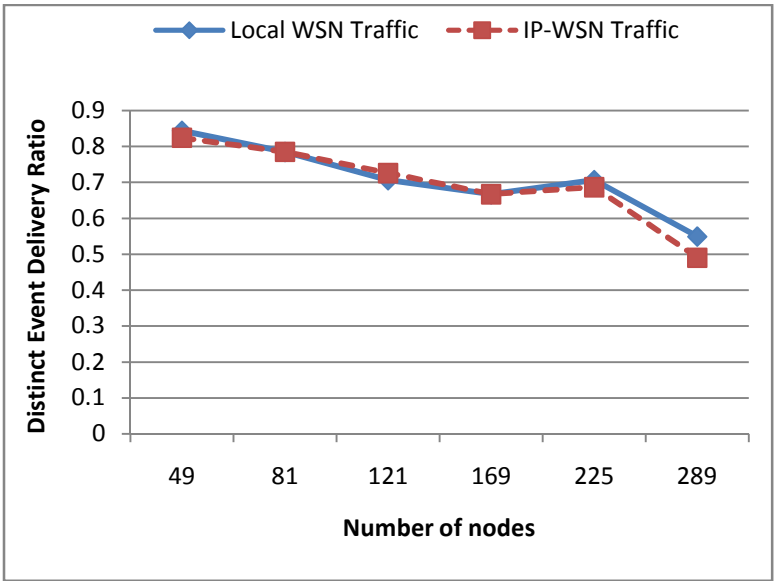


Figure 12. Distinct Event Delievery Ratio in Directed Diffusion

The second experiment tests the effect of the number of interests sent to the network on the performance of the gateway in data-centric mode. The interests are targeting random different nodes scattered over the network. The data reporting interval range from 50 milliseconds to 0.5 second. The refreshment rate of interests ranges from 0.5 to 5 seconds. All interests expire at the end of the simulation. The network size is 11x11 grid of sensor nodes (i.e. 121 nodes). Again, this experiment is run twice. In the first run, a sensor node (i.e. sink) populates the interests to sources. In the second run, multiple of IP hosts are configured to query WSN with the same interests used in the first run. Also, the sink node used in the first run acts as a gateway node in this run to ensure the same network configuration and settings of both runs.

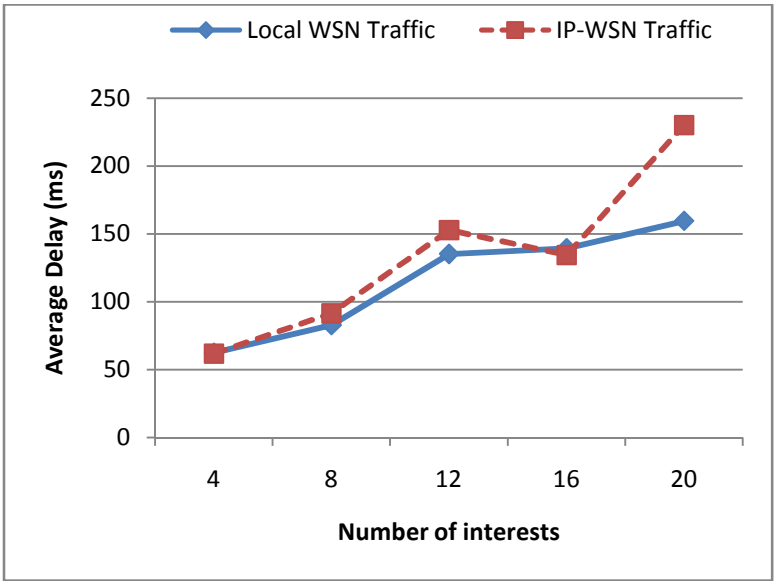


Figure 13. Average Delay with different number of interests

Regarding the interest average delay, results of both runs are compared as shown in Figure 13. The delay of IP-WSN communication is almost the same or slightly greater than local WSN communication

in cases up to 16 interests. In 20 interests' case, the delay of IP-WSN communication is increased greatly. By investigating the details of the experiments, it is found that there are two interests which are successfully received in the second run (IP-WSN) but with high delay. These two outliers increased the average value so much. For this reason, we calculated the median delay for both runs to reinforce our analysis. Figure 14 shows the median delay of both runs. We can see that both became almost the same with minor differences using the median delay instead of the average.

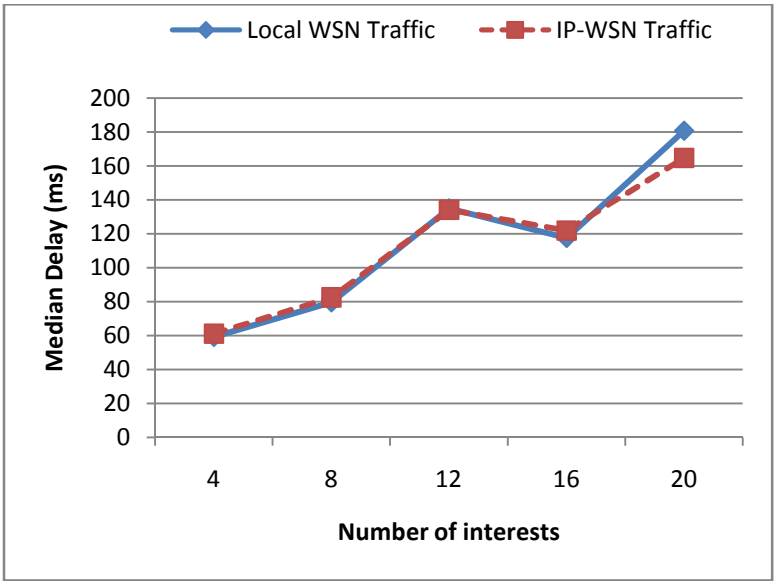


Figure 14: Median delay versus number of interests - data centric WSN

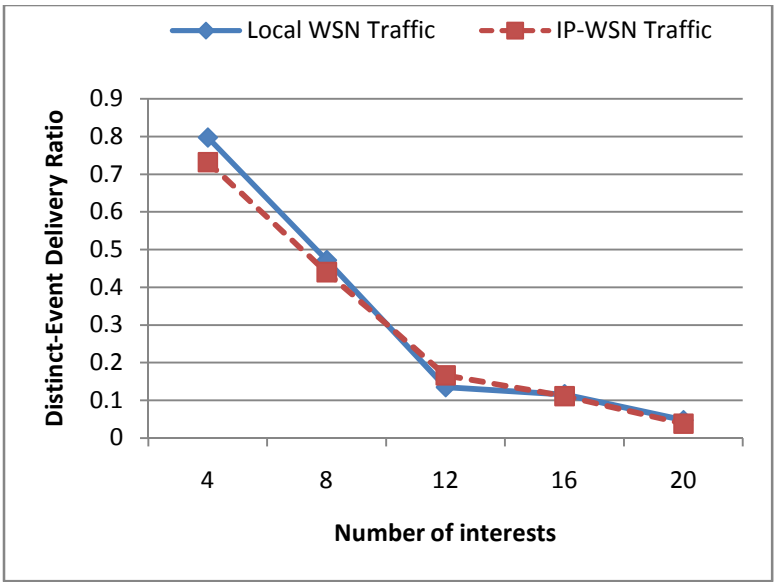


Figure 15. Distinct Event Delivery Ratio with different number of interests

Regarding the distinct event delivery ratio, results of both runs are shown in Figure 15. It is clear that the delivery ratio is decreasing radically with increasing number of interests. This happens due to the huge number of data reporting and interest refreshment packets exchanged continuously among nodes. Also, it is clear that the delivery ratio of IP-WSN traffic is almost the same as the WSN-only traffic. This indicates that the integration does not affect the delivery ratio even with large number of interests.

4. Related Work

As mentioned in section 1, there are two main approaches for interconnecting WSN and IP network; the gateway-based approach and the TCP/IP overlay. Next, the evaluated technique is compared with those approaches.

4.1 Gateway-based Approach

In gateway-based approach, an application layer gateway is used to interconnect between both networks. The gateway can operate in either of two ways: as a front-end proxy or as a relay. In front-end proxy case, the data collected from sensor nodes is stored in a base station connected to IP network (i.e. a proxy server). Then, IP hosts can query this data using SQL or web services. In the second case, the gateway simply relays data comes from sensor nodes to IP hosts. IP clients should register for data interest to receive packets about it [6].
The advantage of this approach is that the protocols of sensor network can be chosen freely to match the application requirements. Also, it can provide security mechanisms for user authentication and authorization. However, it cannot provide direct access to sensor nodes as both networks are completely decoupled. Moreover, it is typically implemented for a specific application task, thus, a special gateway implementation is required for each application. Also, the gateway is a single point of failure. If the gateway is down, all communication between both networks is down [6].
Virtual IP (VIP) Bridge [8] is considered to be a customized method for gateway-based approach. However, it uses a low-level bridge. The evaluated technique in this paper is based on this method. It virtually assigns IPv6 addresses to sensor nodes but it does not assign virtual IDs for IP hosts. It caches received packets in the bridge. When a reply packet reaches to the bridge, it is compared with the cached packets to know which client originally sent this packet. Thus, it adds much overhead in storage and processing to return data packets to IP hosts. VIP Bridge supports the address-centric or location-centric WSNs but not data-centric. Also, its packet translation process depends on specific fields that are not necessary supported in the deployed protocols; and so the running protocols need to be modified to interact with the bridge [2].

4.2 TCP/IP Overlay Approach

In TCP/IP overlay approach, the IP is implemented in sensor nodes for addressing and routing. In [9], a compatible interoperable tiny TCP/IP implementation –called uIP- is implemented for constrained embedded systems such as sensor nodes. In [10], the design of a complete IPv6-based network architecture for wireless sensor networks is presented. The main advantage of overlaying TCP/IP is the direct interoperability with IP hosts without protocol converters or gateways. However, it forces deploying Internet protocol in sensor nodes which may not fit the application requirements. Also, the Internet protocol is address-centric protocol which is not compatible with data-centric WSN. This problem is solved by establishing a tunnel among IP addressable nodes which causes more protocol overhead. On the other hand, it is hard to provide security mechanisms in individual sensor nodes due to their limited resources [1].

4.3 Comparison

Each integration approach has its own merits and drawbacks. In this section, the proposed integration technique is discussed and compared with the other approaches against common design considerations desirable in integration approaches.

Application independent. In direct access to sensor nodes mode, the proposed technique can work with several applications simultaneously as it relays packets received from the IP hosts after simple address translation to sensor nodes. Therefore, no pre-knowledge for the application used is required. However, in data-centric WSN, the WSN application is deployed in the gateway to be able to work with queries. If multiple applications supported in such network, then they should be deployed in the gateway too. The gateway control component must be able to distinct between queries and to forward them according to their applications.

Communication paradigms support. The proposed integration technique supports both address-centric and data-centric WSNs. It so solves the drawback of the original VIP Bridge technique.

Transparency and Consistency. The operations of the gateway node allow transparent communication from one network to the other. The IP hosts can communicate with sensor network, whether address-centric or data-centric, using IP addresses which ensures consistency with NGN as well. Also, in direct access case, the sensor nodes communicate with IP hosts using sensor IDs. This provides transparency to sensor network side too. In data-centric WSN, queries and their replies are forwarded to/from WSN without modification and so the integration technique guarantees full transparency and consistency with NGN.

Security support. The proposed integration technique uses a gateway node for interconnection, so it is a suitable place to apply security rules as all packets go through this node. If the gateway node is not capable enough to perform complex access rules, it can use an external server through its connection to IP network to handle such rules. Thus, the proposed technique supports security mechanisms.

Overhead and modification minimization. As shown in its previous description, the proposed technique does not require any modification in protocols of nodes of either network. This feature is desirable as it gives the flexibility in integration and applicability with diverse WSN protocols. Also, the technique overhead is less than that of application-level gateway as it depends on simple translation and address assignment processes.

Energy efficiency. Using the proposed technique, WSN protocols are chosen freely. Thus, it is possible to select the most suitable protocol for the WSN application in hand which achieves the desired energy efficiency.

Scalability. The proposed technique is scalable and works with dense networks to some extent. By using IPv6 stateless addresses and its auto configuration, the gateway can theoretically addresses any number of sensor nodes. However, it needs a powerful gateway node to handle such large number of nodes along with their traffic. Also, in case of direct accessing, it assigns virtual sensor IDs to IP hosts with lease time control. This ensures efficient utilization for the reserved IDs pool. However, it is still suffer from bottleneck problem as it depends on a single node for communication. This limitation exists

in gateway-based approaches which uses single interconnection node. Table shows a comparison between the integration approaches and the proposed technique.

Table 1: Comparison between proposed technique and the related work

	App-level Gateway	IP Overlay WSN	VIP Bridge	Proposed Technique
Application independent	No	Yes	Yes	Yes[1]
Direct access	No	Yes	Yes	Yes
Data centric support	Yes	Yes	No	Yes
Transparency	No	Yes	Yes	Yes
Security support	Yes	No	Yes	Yes
Minimizing Modification/ overhead	Yes	No	No	Yes
Energy efficient in WSN	Yes	No	Yes	Yes
Scalability	Normal	High	Normal	Normal

5. Conclusion

In this paper, we enhanced and evaluated a framework for interconnection between WSN and IP network. The framework is generic as it supports different WSN architectures such as address-centric and data-centric. It does not require modification or network overlay in WSN or IP network and hence can operate with different applications without adding extra overhead. It consists of two light-weight components that are suitable for non-powerful gateways.

On the other hand, further research is needed to deal with the bottleneck and the single point of failure in the gateway node by supporting multiple gateways and balancing the network load.

REFERENCES

[1] R. Roman and J. Lopez, "Integrating wireless sensor networks and the internet: a security analysis," *Internet Research: Electronic Networking Applications and Policy*, vol. 19, no. 2, 2009, pp. 246-259.

[2] Karim A. Emara; Mohammad Abdeen; Mohammad Hashem, “A gateway-based framework for transparent interconnection between WSN and IP network”, EUROCON 2009, EUROCON ‘09. IEEE, 18-23 May 2009 Pages:1775 – 1780, St. Petersburg, Russia

[3] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: a survey," *IEEE Wireless Communications*, vol. 11, no. 6, pp. 6-28, 2004

[4] Stojmenovic, Ivan Handbook of Sensor Networks - Algorithms and Architectures. (pp: 419). John Wiley & Sons.

[5] C. Intanagonwiwat, R. Govindan and D. Estrin, “Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks,” ACM/IEEE International Conference on Mobile Computing and Networks (MobiCom 2000),August 2000, Boston, Massachusetts

[6] A. Dunkels, T. Voigt, J. Alonso, H. Ritter, and J. Schiller. Connecting Wireless Sensornets with TCP/IP Networks. In Proceedings of the Second International Conference on Wired/Wireless Internet Communications (WWIC2004), Frankfurt (Oder), Germany, February 2004.

[1] In direct access to sensor nodes mode only

[7] Min Zhang, Sangheon Pack, Kideok Cho, Dukhyun Chang, Yanghee Choi, and Taekyoung Kwon, "An Extensible Interworking Architecture (EIA) for Wireless Sensor Networks and Internet," in Proc. Asia- Pacific Network Operations and Management Symposium (APNOMS) 2006 Poster Sessions, Busan, Korea, September 2006
[8] L. Shu, J. Cho, L. Zhang, and M. Hauswirth, "VIP Bridge: Leading Ubiquitous Sensor Networks to the Next Generation", Journal of Internet Technology (JIT), July 15, 2007
[9] Adam Dunkels. "Full TCP/IP for 8-bit architectures". In Proceedings of The First International Conference on Mobile Systems, Applications, and Services (MOBISYS `03), May 2003.
[10] Hui, J. W. and Culler, D. E. "IP is dead, long live IP for wireless sensor networks". In *Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems* (Raleigh, NC, USA, November 05 - 07, 2008). SenSys '08, Pages 15-28. ACM, New York, NY
[11] OMNeT++ Simulator. http://www.omnetpp.org/.
[12] INET Framework. http://inet.omnetpp.org/
[13] Castalia. A simulator for WSNs. http://castalia.npc.nicta.com.au/