Implementation of TCP/IP Protocols in Wireless Sensor Networks

Mirko R. Kosanovic[1] and Mile K. Stojcev[2]

Abstract – **Wireless Sensor Networks (WSNs) are large networks composed of small sensor nodes with limited computer resources capable for gathering, data processing and communicating. WSNs usually can not operate in isolation, i.e. they have to be connected to some Wide Area Network (WAN). As the Internet protocol becomes de-facto standard for WANs, it is a challenge now to connect WSNs to WAN through TCP/IP protocol. In this paper we will analyze, first, the current well known solutions, which relate to connecting WSNs to TCP/IP based networks. In order to make WSN transparent to TCP/IP networks, we involve local node addressing within the WSN. By using this approach the traffic density between sensor nodes and the access point is decreased. In order to evaluate performance of the communication we define a traffic reduction factor $\Phi(m,h)$ as a metric. For several messages and hops we point to the effects of the decreased traffic that can be achieved using the proposed method.**

Keywords – **TCP/IP, Wireless Sensor Networks, Internet**

I. INTRODUCTION

Wireless sensor networks are composed of a large number of radio-equipped sensor devices, that autonomously form a network, through which sensor nodes are capable of sensing, processing and communicating among each other. Some crucial properties of WSNs are the following: a) nodes are densely deployed in a region and are very often prone to failures; b) broadcast communication paradigm, mainly used without global identification (ID), is implemented; c) nodes operate under limited power; and d) computational capacity and memory space of each sensor node is limited, too. In general, WSNs do not work efficiently in full isolation. So, it is imperative to connect them to some other kind of networks, such as Local Area Network (LAN), Metropolis, WAN and Internet. In this way very complex heterogeneous distributed network (HDN) can be configured. Such connection, from one side, provides transparent operation of the WSN for all HDN`s end users, but, from other side, creates new challenges related to the development and research in this field. Having in mind that TCP/IP protocol suite becomes de-facto standard in network connectivity, it is quite reasonable to look at some efficient methods for interconnecting protocol specific WSN to TCP/IP based network, such as for example Internet. This problem is in focus of our interest in this paper. At the start, a short survey related to current researches on this field will be given. Next, in order to evaluate communication performance of the WSN-TCP/IP-middleware we define a traffic reduction factor. After that, we propose a method for traffic reduction between WSN and TCP/IP based network. Finally, for several messages and different number of hops we present results obtained by implementing the proposal.

[1]Mirko R. Kosanović is with the High Technical School, A.Medvedeva 20, 18000 Nis, Serbia, E-mail: vkosanovic@sbb.co.yu
[2]Mile K. Stojcev is with the Faculty of Electronic Engineering, A.Medvedeva 14, 18 000 Nis, Serbia, E-mail: stojcev@elfak.ni.ac.yu

II. APPLICABILITY OF TCP/IP PROTOCOLS IN WSNs

With the rapid development of wireless technology, the increased requirements for implemmentation of TCP/IP based networks become a necessity. To solve this problem efficiently is not an easy task, especially in WSNs, where sensor nodes (SNs) are realized with many limited resources. Without doubth, one of the more pronounced design challenge relates to SN's power consumption. Namelly, since the energy of the battery powered SN is limited, in order to prolong it's live, micro power consumption for SN is of paramaunt importance. Numerous researches conveyed in this field [4], [5], [6], [7] show that the communication building block is the largest energy consumer of the wireless SN. For example, the energy which is consumed to send only one bit of data is less or equivalent than the amount of energy needed to process 100 instructions for Berkely node [1]. The TCP/IP protocol is often perceived to be „heavy-weight" protocol, because, as a first, its implementation requires large amounts of resources both in terms of memory and processing power, and as a second, the size of its header is too large (IPv4-24 byte, IPv6-40 byte, UDP-8 byte, TCP-24 byte). Having this in mind, a direct implementation of TCP/IP protocol in WSN results to an inefficient design solution, i.e. we have to send 30 bytes of message for only 2-3 bytes of useful payload data. To cope with this problem several methods have been proposed [7], [8], [9].

II.1 Communication models

WSNs use the following three types of communication models:

1. Adress-Centring communication – in this case all sensor nodes have an unique ID number and the routing is performed according to IDs. This kind of protocols, is referred as table-driven routing protocols [2].
2. Data-Centring communication – sensor nodes are without ID numbers. Communication is based on broadcast messages. There are two kind of messages: *Interest packet*, which propagates an information interest through the network, and *Advertisement packet* which is replay from sensor nodes on which an interest has been registered [3].
3. Location-Centring – sensor nodes use the location as a primary means for addressing and data routing. Each

sensor node has an unique spatial address which depends of its physical location in the deployed region..

If we analyze the communication possibilties of all three models and try to implement these models in TCP/IP network, we can conclude the following: Data-Centring model is not good candidate for TCP/IP networks. In order to provide consistency between WSN and TCP/IP, the Address-Centric and Location-Centring communication paradigms are better solutions for interconnecting WSNs and TCP/IP networks [4].

II.2 Communication architecture

According to the communication architecture, we divide the communication methods (see Figure 1.) as those that are based on: Proxy architecture, Overlay based architecture and Gateway architecture.

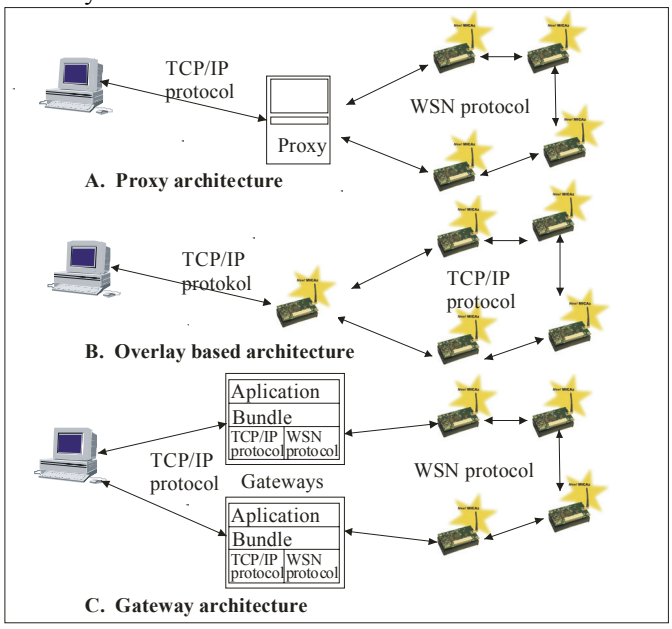

Fig. 1. Three types of communication architectures

II.2.1 Proxy architecture

The comunication between TCP users and sensor nodes is done through the proxy computer. The communication protocol used in the sensor network may be chosen freely. There are two various modes according to which proxy can be operative and can interconect WSN with TCP/IP networks as:

1. *relay* – in this mode all data which are coming from one network are passed to the another network.
2. *front-end* – the proxy pro-actively collects data from sensor nodes and stores this information in its database. The users from TCP/IP networks can query for specific data in a variety ways, such as SQL queries or WEB based interfaces.

Both solutions have some drawbacks, what make these solutions not applicable in general. As a first, a single point of failure exists. When the proxy stop working, all communications to and from the WSN are broken. As a second, the proxy implementation usually depends on the specific task or a particular set of protocols. This means that for each application different proxy is needed.

II.2.2 Overlay based architecture

There are two kinds of overlay based methods: *TCP/IP overlay sensor networks*, and S*ensor networks overlay TCP/IP* [5]. The first approach points that it is possible to implement TCP/IP protocol stack to microcomputer system with very poor resourses: 8-bit microprocesor with only 2kB RAM memory [2]. In *Sensor networks overlay TCP/IP* the protocol stack of WSN is deployed over the TCP/IP stack and each Internet user is considered as a virtual sensor node. The virtual sensor node can interpret WSN packets since it has installed the WSN protocol stack in addition to TCP/IP stack. Numerous problems accompany the implementation of TCP/IP in WSNs. They can be identified as: header overhead, high bit error rates, high energy consumptions for end-to-end multi hop retransmissions, differences in routing protocols and implementation of adressing and routing schemes [4].

II.2.3 Gateway architecture

One of the essential device who provides a connection between wireless and TCP/IP network is a gateway. It performs several tasks such as protocol conversion, message delay,etc. All solutions, that use gateway as an interconecting device, can be grouped into the following two categories: *Aplication gateway* and *Delay Tolerant Network (DTN)*. Aplication gateway is a simple gateway based approach which works in aplication layer [9]. The DTN, is a similar solution. The main difference in respect to *Aplication gateway* is the following: It implements one new layer, both in TCP/IP and WSN networks, referred as *Bundle Layer*. The main function of the bundle layer is to store and forward packets beetwen two network (Figure 1.).

III. A GATEWAY AS A TCP/IP TO WSN ADDRESS TRANSLATOR

Main design challenges concerning the interconection between TCP/IP based networks and WSNs are related to the fact that it is neccessary to provide: a.) access to each SN through the TCP/IP based network; b.) efficient communications from aspect of SN's energy consumption; and c.) transparency in operation between TCP/IP based protocols and WSN protocols.

The method which we propose in this paper is sutiable for applications area such as: health monitoring (diagnostics, telemonitoring), environmental monitoring (fire detection, water pollution, tracing movements of birds, animal or insects, detection of chemical and biological agents), military and security (movements of soldiers and vehicles, monitoring critical terrain), industrial process control, smart buildings, traffic control, etc. In general, both from aspect of toplogical hierachical network organization, from one side, and control, from other side, these systems are heterogeneous in nature. Therefore, in order to design an optimal solution, for a particular case, it is neccessary first to forsee the curcial assumptions and requirement that these kinds of networks have to fulfill:

- WSN is organized as set of clusters.
- Cluster topology is aribritrary.
- Each cluster is organized around one Main Sensor Node, referred as a MSN.

- The MSN acts as a gateway between the WSN and TCP/IP based network.
- To each MSN two addresses are appended. The first one is TCP/IP address, while the second is local WSN's address.
- SNs can accsess to TCP/IP users through MSN, or contrary.
- Within each cluster, it is possible to address 255 single-addressed SNs, 128 double-addressed SNs, 64 quad-addressed SNs, etc.
- The number of addresses appended to each SN determines the number of messages with which the SN can manipulate simultaneosly, i.e. at the time.
- For data transfer, store and forward technique is used.
- Single hop and multi-hop data transfers whitin the cluster are possible.
- During the initialization phase, the MSN assigns different group of addresses (single, double, quad, octal etc.) to each SN, according to the predicted traffic intensity among SNs and MSN.
- To the TCP/IP users each SN is visible through its first group address.
- MSN can transfer data to: a.) SNs located within single cluster area; b.) to MSNs that are constituents of other clusters; and c.) to TCP/IP users.

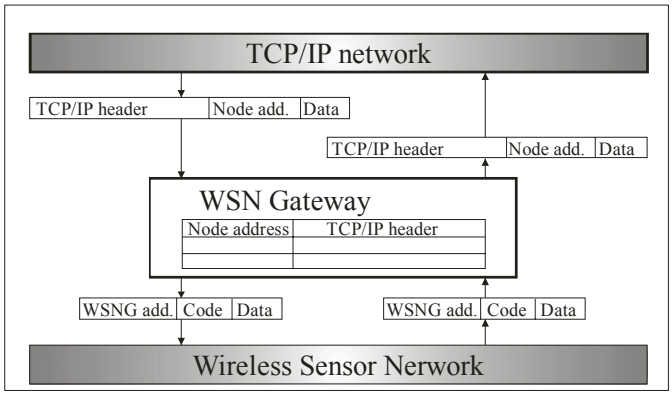

Fig. 2. Translation table

Figure 2. depicts the principle of messages transfer between TCP/IP network and WSN. As can be seen from Fig.2 the MSN acts as a protocol translator between both networks. From software piont of view it maps addresses from one network domain to another, and translates larger TCP/IP header into smaller WSN header. In order to perform this activity it uses data stored in a translation table.

The translation table has 256 entries. Each entry has two fields. The first field points to the SN's local address, while the second to the TCP/IP header. For single addressed SN one table entry is appended, to double addressed SN two table entries are appended, etc. This kind of table organization allow us to direct several TCP/IP messages to the same SN at the time, without extending the WSN header. Smaller header sizes directly implies to lower communications cost, and indirectly to decreased energy consumption of the SN.

IV. A GATEWAY: PRINCIPLE OF OPERATION

In order to evaluate the performance of the proposed solution we have assumed the following: a.) each SN within a cluster is seen as TCP/IP addressible unit; b.) protocols above and bellow the network layer remain unchanged; c.) data transfer between two communication units is store-and-forward type; d.) single hop or multihop are allowed; e.) all data transfers are error free, i.e. without retransmissions. Successible data transfer of one message between two SNs (message transfer and responce) depends of the shortest end-to-end delay. This kind of communication delay includes the following items:

1. T_t (transmission delay) – time for transmition one message It depends on the channel bandwidth, bit rate, message length, and coding technics.
2. T_p (propagation delay) – signal propagation time between two SNs.
3. T_c (processing delay) – the time needed for processing one message.
4. T_q (queueing delay) – an averge time during which message wait in a queue for transmission.

The total communication time for the solution given in reference [4] is defined as:

$$Tref = 2mh(2Tc + Tt + Tp) + 2m(h-1)Tq \qquad (1)$$

while for the solution proposed in this paper is:

$$Tps = 2(m+1)hTc + 2(m+h-1)Tt + 2hTp + 2m(h-1)Tq \qquad (2)$$

where m is a number of transfered messages, and h coresponds to a number of hops. In Figure 3A. the principle of single message data transfer among four SNs is pictured. Figure 3B. corresponds to data transfer of four messages. Let note that overllaping between data transfers in this case exist.

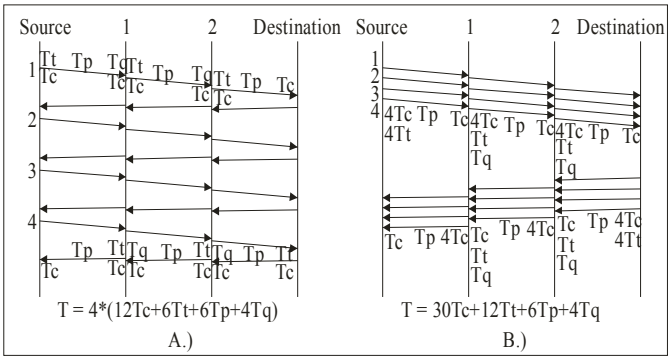

Fig. 3. Time needed for transmission of four messages

In order to evaluate the performance of both proposal we assume the following:

1. the data transfer rate is R = 720 kbps,
2. one WSN message usualy consists of N = 16 bytes,
3. the signal propagation velocity is $v_p = 3*10^8$ m/s,
4. the distance between SNs is uniform, and is within a range d = (10-150) m,
5. CPU clock frequency is f = 12 MHz and the average number of instruction to process one byte is n = 10 instructions with t = 4 clock periods per instruction.

According to the invoved assumptions and by substituting these values into T_c, T_t and T_p we obtain:

$$Tt = N / R = 16*8/720\,kbps = 173{,}6\,\mu s \quad (3)$$

$$Tp = d / v_p = 0{,}1\,\mu s \text{ for } d = 30\,m \qquad (4)$$

$$Tc = N * n * t / f = 16 * 10 * 4 / 12 = 53{,}33\,\mu s \qquad (5)$$

For traffic without retransmissions $Tq = 0$

Having in mind that $T_t >> T_p$ and $T_c >> T_p$ we can ignore T_p and T_q in respect to T_p and T_c, respectively. We will involve now a new metric $\Phi(m,h)$ called trafic reduction factor. The metrics $\Phi(m,h)$ is defined as a ratio between the total communication time defined in our porposal and the total comunication time defined in Ref. [4]. This metrics points to the percentage of decreasing the total commuication timesT_{ps} in respect to T_{ref}, in terms of number of messages m, and number of hops h, as parameters.

$$\Phi(m,h) = \frac{Tps}{Tref} = \frac{mh + h + \frac{Tt}{Tc}(m + h - 1)}{2mh + \kappa mh} \qquad (5)$$

By substituting the values for T_t=173,6 ms and T_c=53,33 ms we define $T_t/T_c \approx 13/4$. Accordingly (5) we obtain:

$$\Phi(m,h) = \frac{Tps}{Tref} = \frac{4mh + 17h + 13m - 13}{21mh} \qquad (6)$$

Figure 4. sketches the metric Φ in terms of m, with h as parameter. As can be seen from Fig.4 by increasing m and h, the metric $\Phi(m,h)$ decreases what means that our proposal has better performance (from 14% for m=4 and h=1, up to 50% for m=4 and h=4). Let known that further hop increases (h>=5), does not result a linear $\Phi(m,h)$ decrease.

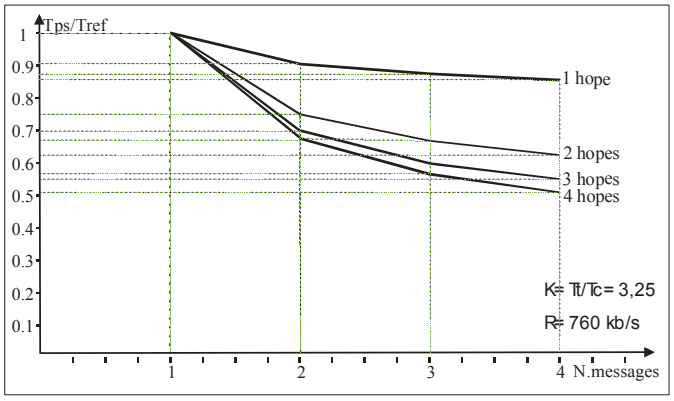

Fig.4 Metric $\Phi(m,h)$ in terms of m with h as a parameter

Figure 5. presents the metric $\Phi(m,h)$ in terms of h, with m as parameter. By analyzing Fig.5 we can conclude that for larger messages (m>=2) the metric $\Phi(m,h)$ decreases what implies that our proposal has better performance in respect to the Ref.[4] (from 10% for m=2 and h=1, up to 49% for m=4 and h=4).

V. CONCLUSION

The problem of impementation of TCP/IP protocols in WSNs is considered. This possibility allow us to access each sensor node as an TCP/IP addressable unit. In order to decrease the node access time and to pertain standard WSN protocol in a process of addresses mapping, we have involved within the gateway architecture a translation table which can

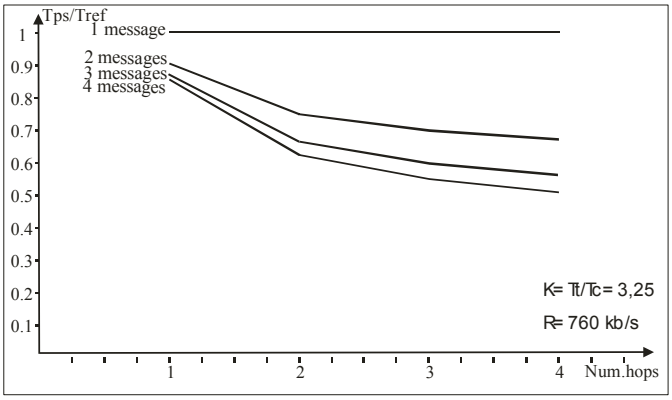

Fig.5 Metric $\Phi(m,h)$ in terms of h with m as a parameter

provide multiple node addresses for a single sensor node. In this manner we have decreased the number of bytes in WSN message header and increased data transfer efficiency. In order to evaluate the performance of our proposal we have involved a metrics called traffic reduction factor. The obtained results, that performace improvement during message transfer among sensor nodes in WSN up to 50 %, in respect to the solution proposed in Ref.[4], are obtained.

REFERENCES

[1] M.Zuniga, B.Krishnamachari, ''Integrating Future Large-scale Wireless Sensor Networks with Internet'', www.cs.usc.edu/Research/techreports/papers/03-792.pdf

[2] A.Dunkels, ''Towards TCP/IP for Wireless Sensor Networks'',Malardalen University Licentiate Thesis No. 45, Swedish Institute of Computer Science, March 2005.

[3] C.Intanagonwiwat, R.Govindan, D.Estrin, ''Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks'', Proc.ACM MobiCom'00, Boston, MA, 2000, pp. 56-67

[4] S.Lei, W.Xiaoling, Xu Hui, Z.Jie, J.Cho, S.Lee, ''Connecting Heterogeneous Sensor Networks with IP BasedWire/WirelessNetworks'',SEUS-WCCIA`06,2006

[5] H.Dai, R.Han, ''Unifying Micro Sensor Networks with Internet via Overlay Networking'', Proc.IEEE Emnets-1, Nov, 2004

[6] K.Mayer, W.Fritsche, ''IP-enabled Wireless Sensor Networks and their integration into the Internet'', http://portal.acm.org/ft_gateway.cfm?id=11426878&type=a5-mayer.pdf

[7] M.Zhang, S.Pack, K.Cho, D.Chang, Y.Choi, T.Kwon, ''An Extensible Interworking Architecture (EIA) for Wireless Sensor Networks and Internet'', www.mmlab. snu.ac.kr/publications/docs/EIA_APNOM2006.pdf

[8] C.Westphal, ''Layered IP Header Compression for IP-enabled Sensor Networks'', www.people.nokia.net/cedri c/Papers/icc06.pdf

[9] Z.Z.Marco, K.Bhaskar, ''Integrating Future Large-scale Wireless Sensor Networks with Internet'', www.cs.usc.edu/Research/techreports/papers/03-792.pdf