American Journal of Computer Science and Engineering
2015; 2(2):5-9
Published online February 10, 2015 (http://www.openscienceonline.com/journal/ajcse)

Security of Wireless Sensor Networks for Monitoring System

Salah Talha Babiker, Abdel Fatah M. Bashir

Computer Engineering Department, University of Taif, College of Computers & IT, Taif City, Kindom of Saudi Arabia

Email address

s.idrees@tu.edu.sa (S. T. Babiker)

To cite this article

Salah Talha Babiker, Abdel Fatah M. Bashir. Security of Wireless Sensor Networks for Monitoring System. *American Journal of Computer Science and Engineering*. Vol. 2, No. 2, 2015, pp. 5-9.

Abstract

Wireless Sensor Networks (WSN) is an interconnection of a large number of nodes deployed for monitoring the system by means of measurement of its parameters. Recent research in wireless sensor networks has led to various new protocols which are particularly designed for sensor networks. To design these networks, the factors needed to be considered are the coverage area, mobility, power consumption, communication capabilities etc. These networks are likely to be composed of hundreds, and potentially thousands of tiny sesor nodes, functioning autonomously, and in many cases, witnhout access to renewable energy resources. Cost constraints and the need for ubiquitous, invisible deployments will result in small sized, resource-constrained sensor nodes. While the set of challenges in sensor networks are diverse, we focus on security of Wireless Sensor Network in this paper. We propose some of the security goal for Wireless Sensor Network. Further, security being vital to the acceptance and use of sensor networks for many applications.

Keywords

Wireless Sensor Network, Applications, Design Issues, Routing Protocols, Simulator Tool and Security

1. Introduction

Sensor nodes are the network components that will be sensing and delivering the data.Depending on the routing algorithms used, sensor nodes will initiate transmission according to measures and/or a query originated from the Task Manager. According to the system application requirements, nodes may do some computations. After computations, it can pass its data to its neighboring nodes or simply pass the data to the Task Manager.

The sensor node can act as a source or sink/actuator in the sensor field. The definition of a source is to sense and deliver the desired information hence, a source reports the state of the environment.In Wireless Sensor Networks (WSN), most of a sensor's energy is consumed for channelsensing and data transmission. Due to the broadcast nature of the wireless medium, a sensor consumes energy for sensing every packet transmitted by its one-hop neighborsLikewise, a sensor consumes energy for the transmission of raw monitored data

In order for wireless mesh networks to be able to self-configure to adapt to changing operationalconditions, it is necessary for the nodes to be able to sense the environment in order to determine the operational state of the system. The state is then used to compare against potential optimization outcomes. In this paper we consider both nodes that participate in network access infrastructure as well as wireless sensor nodes which form part of a future Internet of things infrastructurescenario. We therefore focus on two aspects of the sensing, first, channel state sensing for determining configuration actions which will improve network capacity and lower delays and second, sensing of the environment for data management in sensor networks. This work also includes security aspects of data management in these networks.

Security is a major concern for a large fraction of sensor network applications. The components and operations between sensor nodes within the sensor field would be explored. We first describe the wireless sensor network architecture and the communication protocols for the wireless sensor network. This is essential to understand the hardware and software level power savings strategies.

2. Architecture-Level Optimizations

Once deployed, sensor networks have no human intervention. The nodes themselves are responsible for reconfiguration in case of any changes. Therefore, it is important to select. Appropriate sensor node to suit the application. In this paper we focused on sensor networks design like routing, MAC design, and sensor nodes deployment. In thosedesigns, sensor data are transmitted to remote server through access devices. Tasks like sensor data storage, and notifications are conducted by a central server while gateway onlyacts as an intermediate device. The response delay includes network delay and central server delay. For example in fire system, WSNs provide a large quantity of real-time signals which should be processed in time.With the increase number of patientsand injurts , central server's processing time will increase rapidly. The long distancedata transmission may also cause problems, such as congestions and packet losses. With the advances inelectronics technique, current embedded systems have much faster processor and bigger memory. This allowsthe gateway to have the ability to complete some more complex works and to interconnect to different kinds of public networks. To solve the problems above, we have designed a gateway-centered WSN for geralpurpose system.In this gateway, some tasks are moved to the gateway to reduce the burden of remote server and public networktraffic. In this paper, the hardware and software has been designed with the WSN and a remote server. An onboard Data Decision System (DDS) has been designed to make a decision of the cases studies.

In WSN, the main task of a sensor node is to sense data and sends it to the base station in multi hop environment for which routing path is essential. For computing the routing path from the source node to the base station there is huge numbers of proposed routing protocols exist [8]. The design of routing protocols for WSNs must consider the power and resource limitations of the network nodes, the time-varying quality of the wireless channel, and the possibility for packet loss and delay.

This paper presents a wireless sensor network for the surveillance of critical areas. Provides several protocols that ensure the secure detection of of sensor nodes. Protocol performance was investigated first by an extensive set of simulations in different scenarios. Currently the tested is being extended for further outdoor experiments and to test the protocols in larger real-world

We try to address these requirements into our proposed design, so here we suggest a framework of smart algorithms. and structure model which can mange with large number of sensor nodes planned for many applications also implies a major portion of these networks would have to acquire self organization capability.Intuitively, a denser infrastructure would create a more effective sensor network. It can provide higher accuracy and has more energy available for aggregation. If not properly handled, a denser network can also lead to collisionsduring transmission, and network congestion. This willno doubt increase latency and reduce efficiency in terms of energy consumption. One sensing, communication and computation. Unlike the Internet, where data generation is mostly the province of end points, in sensor distinguishing characteristic of WSNs is their lack of strong boundaries between networks every node is both a router and a datasource.

Gateways allow the scientists/system managers to interface from their personal computers (PCs), personal digital assistants (PDAs), using Internet and existing network protocols. In a nutshell, gateways act as a proxy for the sensor network on the Internet. According to gateways design can be classified as active, passive, and hybrid. Active gateway allows the sensor nodes to actively send its data to the gateway server. Passive gateway operates by sending a request to sensor nodes. Hybrid gateway combines capabilities of the active and passive gateway. (See Figure 1).

As shown in Figure 1, the wireless sensor network and the classical infrastructure comprises of the standard components like sensor nodes (used as source, sink/actuators), gateways, Internet, and satellite link, etc.

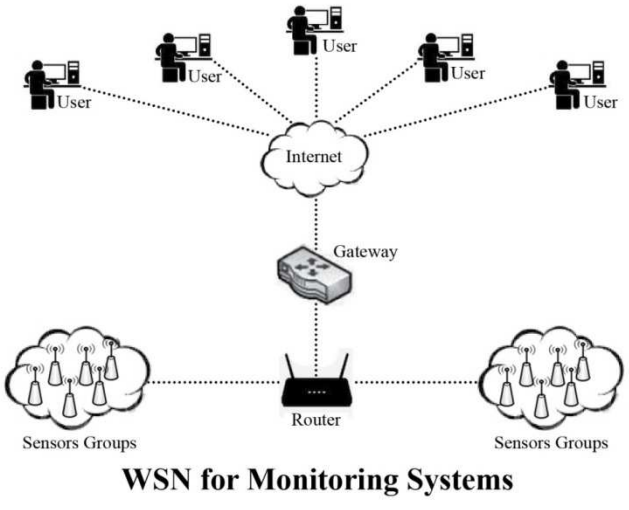

Figure 1. *WSN for Monitoring Systems*

3. Wireless Sensor Network

A wireless sensor network (WSN) is a wireless networkconsisting of spatially distributed autonomous devicesthat use sensors to monitor physical or environmentalconditions. These autonomous devices, or nodes, combine with routers and a gateway to create a typicalWSN system. Sensor networks are the key to gatheringthe information needed by smart environments, whetherin buildings, utilities, industrial, home, shipboard,transportation systems automation.

A sensor network is required that is fast and easy to install and maintain. The smart gateway isdesigned to enable WSN and public communicationnetworks to access each other easy way. In this paper , the gateway consists of central control unit, database (DB), WSN module,WLAN AP, and GSM module, as mentioned in Figure1.The distributed measurement nodes communicatewirelessly to a central gateway, which provides aconnection to the wired world where the data can be collect, process, analyze and present your measurementdata. To extend distance and reliability in a wirelesssensor network, we propose using routers to gain anadditional communication link between end nodes and the gateway. The gateway includes three externalcommunication modules (ECM): WSN Module, WLANAP, and GSM Module. WSN module, on one hand, ismainly used for receiving data packages from the sinkof the WSN; on the other hand, it is used to sendcommands to the Task manger .A GSM module is needed when sending SMS the gateway can access throw IP connections to internet cepts the IP address assignedby the internet server. Second, it sets up an ad-hocnetwork for care-givers and system maintainers so that they can connect to the smart gateway with laptop orPDA easily.

4. Security

Douceur first introduced the notion of Sybil attack [4], where a single entity (node) illegitimately presents multiple identities. As the nodes in sensor networks can be physically captured by an adversary, sybil attack can manifest in a severe form leading to the malfunction of basic operational protocols including routing, resource allocation and misbehavior detection. In this paper we propose a location verification based defense against attackers specialy Sybil attack.

5. Definition of Sybil Attack

We try to give ashort definition of Sybil Attack, an attacker create Sybil nodes and use them in two ways direct and Indirect communication in direct communication legitimate nodes can communicate with Sybil nodes directly.In the indirect communication one or more of the malicious devices claims to be able to reach the Sybil nodes, that messages sent to a Sybil node are routed through one of these malicious nodes. Attacker also can used Stolen Identities (Fabricated) which assign other legitimate identities to Sybil nodes.The same identity is used many times and exists in multiple places in the network, depending on the number of these identities the attacker may be able to determine the Outcome of any sensor. Security should be implemented in the system by Keeping information private by encrypting data [2] Authenticate data communication [3] making it not possible to interfere with transmitted signals. The more security a system has the more power and bandwidth are spent. For some applications it is important to make a trade-off between security and network resources.

5.1. Proposed Framework

Key design issue of this network architecture is the development of a new approach of framework to do what? to calculate the optimal assignment of renewable energy supplies to maximize lifetime of wireless sensors network, obtaining the minimum number of energy supplies and their node assignment. We also conduct a second optimization step to additionally minimize the number of packet hops between the source and the sink

The deployment of large-scale sensor presents various challenges whose solution requires the design and development of power-and-time efficient Algorithms. In this paper many proposals and various standards have suggested the use of time division multiple access (TDMA) in order to guarantee tight-time scheduling and high overall network throughput under high load conditions. However, in TDMA networks the time and overhead required during the setup phase are major drawbacks that are often overlooked. In this paper we introduce a simple and robust algorithm specially tailored to be used during the setup phase of a TDMA-based WSN.As a case study, we consider the setup phase of the synchronous protocol SA-MAC. Our results show that the proposed algorithm is able to configure highly populated networks in significantly shorter times than traditional CSMA/CA. Furthermore, an experimental prototype has been developed allowing us to show the Minimizing Schedule Length: Minimizing the schedule length, or equivalently, minimizing the time to complete convergecast, is the most-studied design objective for data collection in sensor networks. It translates to quicker data collection at a fast rate. In many WSN applications, it is of interest to maximize the rate at which the sink can receive data from the network For instance, it is noted that in networked structural health monitoring, more than 500 samples per second are required to efficiently detect and localize damages Secondly, a minimal-length TDMA schedule allows for a longer sleep period in each data collection cycle, especially for periodic traffic, which contributes to lesser energy consumption on the sensor nodes. Minimal schedule length can be achieved by maximizing the reuse of the time slots. Therefore, most of the existing algorithms aim to maximize the number of concurrent transmissions and enable spatial reuse by devising strategies to eliminate interference. [6]

This paper presents a fast algorithm which guarantees energy-efficient data collection by Wireless Sensor Networks

(WSNs) under delay constraints. Present Medium Access Control (MAC) protocols in WSNs typically sacrifice packet latency and/or the reliability of packet transfer to achieve energy-efficiency. Thus, the paper is concerned with developing a novel protocol to achieve energy efficient and reliable multihop data transfer in WSNs satisfying given latency requirements. Energy efficiency is achieved by optimizing the scheduling of the underlying Time Division Multiple Access (TDMA) system by minimizing the wake-up number of the nodes. Schedule optimization is transformed into a quadratic programming (QP) task, which is then solved by the Hopfield net in polynomial time. In this way, an energy efficient scheduling can be obtained which meets a given delay requirement in TDMA systems. The performance of the new algorithm has been evaluated by simulations and compared to the performance of well-known scheduling methods, such as SMAC, UxDMA [8] (a slot assignment algorithm for WSN), and traditional tree-based protocols. The simulations have demonstrated that our method reduces global power consumption for time-driven monitoring. Wireless Sensor Networks (WSNs) are capable of conveying high-resolution information processes to a Base Station (BS) However, the longevity of such networks has become of crucial importance in applications like environment and health monitoring, where WSNs might have to be operational for several years Therefore one of the most important problems of WSNs stems from the limited energy storage capacity which imposes severe limits on the longevity The major energy consumption of a sensor node results from the active state of its radio component Thus, by “sleeping” (i.e., switching off the radio module), one may save a considerable amount of energy Therefore the lifespan of a wireless network is roughly defined by how often the electricity consuming parts are turned on. In WSN, the physical layer was designed with short radio range to meet the requirement of low energy consumption. As a result, the network frequently relies on multihop communication schemes to the BS but this procedure leads to asymmetry in the energy consumption; nodes close to the BS are forced to be engaged in higher forwarding activity Existing routing approaches of load and energy balancing

5.2. Security Keys & Cryptographic

Study of cryptographic primitives and security protocols for wireless sensor networks, including an energy analysis of various public-key cryptosystems like RSA and DSA. They found out that the energy cost for generating similar signature. Our evaluation of key establishment protocols considers both the energy that the Model consumes during the execution of cryptographic algorithms and the energy cost of radio communication. We used the energy characteristics

of the nodes ,upon which the node’s average power consumption that let the processor be active. The energy required for the calculation of cryptographic Primitives is simply the product of the average power consumption and the execution time. We determined the execution time of the cryptographic primitives through the simulations process

6. Related Work

Multi-channel MAC protocols have been extensively studied for wireless ad-hoc network [7] However, there are some key differences between these existing protocols for traditional wireless ad-hoc network and the channel allocation protocols proposed in this paper for WSN as detailed below. First, the protocols in [9], assume that the hardware is able to listen to multiple channels simultaneously. But each sensor device is usually equipped with a single radio transceiver that cannot transmit and receive at the same time, and cannot operate on different channels simultaneously. Second, the protocols in involve heavy centralized computation such as linear programming and each sensor device has limited memory and limited processing power (8MHz MSP430 microcontroller in TelosB motes), making a WSN unsuitable for such heavy-weight computations.

7. Conclusions

In this paper, the design method for a monitoring applicationsystem using a wireless sensor network (WSN) is proposed. This paper has successfully demonstrated the application of the WSN to monitor a vary of objects (fire system, gas detection, car movement survellance etc). Programs for simulations have demonstrated that our method reduces global power consumption for time-driven monitoring. Algoritms are developed using Multi-channel MAC protocols, also successfully demonstrated to possess good performance in data collection, monitoring, control and display fat informations.

References

[1] V. Arnaudov, “Unified Management of Heterogeneous Sensor Networks In the Atlantis Framework”, Department of Computer Science, Brown University. S. Tilak, N. Abu-Ghazaleh, and W. Heinzelman, A taxonomy of Wireless Micro-senor Network Models, ACM SIGMOBILE, Mobile Computing and Communications Review, vol.6, issue: 2, pp. 28-36, April, 2002. [Available from the World Wide Web (WWW): http://www.cs.binghamton.edu/ nael/research/papers/taxonomy.pdf].

[2] J. N. Al-Kamal, and A. E. Kamal, Routing Techniques in Wireless Sensor Networks, A survey, Wireless Communications, IEEE, vol. 11, pp. 6-28, 2004. [See also IEEE Personal Communications].

[3] D. Puccinelli and M. Haenggi, “Wireless sensor networks: applications and challenges of ubiquitous sensing,” IEEE Circuits and Systems Magazine, vol. 5, no. 3, pp. 19–31, 2005.K. Akkaya, and M. Younis, A survey on Routing Protocols for Wireless Sensor Networks, Elsevier Ad Hoc network Journal, vol.3, pp.325-349, 2005.

[4] K. Holger, W. Andreas,A short Survey of Wireless Sensor Networks, Technical Report [TKN Technical Report TKN-03-018], Berlin, October, 2003. [Available: http://www.tkn.tu-berlin.de/publications/papers/ TechReport03018.pdf].

[5] A.A. Ahmed, H. Shi, Y. Shang, A Survey on Network Protocols for Wireless Sensor Networks, In Proc. of International Conference on Information Technology: Research and Education (ITRE03), pp. 301 - 305, 11-13 Aug. 2003.

[6] D. Braginsky, D. Estrin, “Rumor Routing Algorithm for Sensor Networks”, Proceedings of the First Workshop on Sensor Networks and Applications (WSNA), Atlanta, GA, October 2002.

[7] S. C. Ergen and P. Varaiya, “TDMA scheduling algorithms for wireless sensor networks,” Wireless Networks, vol. 16, no. 4, pp. 985–997, 2010.

[8] Sharma and S K Jena, "A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks", ICCCS’11 February 2011.

[9] Fan, S., Zhang, L., Ren, Y.: Approximation algorithms for link scheduling with physical interference model in ireless multi-hop networks. CoRR abs/0910.5215 (2009).

[10] Raymond, R.C. Marchany, M.I. Brownfield, and S.F. Midkiff. Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols. IEEE Transactions on Vehicular Technology, vol. 58, no. 1, pp. 367-380, 2009.