European Online Journal of Natural and Social Sciences 2015; www.european-science.com
Vol.3, No.3 Special Issue on New Trends in Architecture, Civil Engineering, and Urban Studies
ISSN 1805-3602

Designing a security unit to reduce the permeability of anonymous groups and congestion control in wireless sensor networks

Ahad Zare, Mehdi Pourhasan, Tahereh Sotudeh
Department of Mechatronic Engineering, Islamic Azad University, Ahar Branch

Abstract

Recent developments in the fields of electronics and wireless communication have provided conditions to design and build lower power consumption sensors and use of radio signals for information communications has provided various applications. Design of such networks has their own specific challenges. One of these problems is the probability of congestion due to higher data transmission rate. Using radio signals, the hackers are able to pretend and introduce themselves as a network member through cracking security barriers and in this case the conditions are provided for hacker nodes to access critical information and other destructive activities. Hence, in this paper we will present a new algorithm for the problem of congestion and increase of security in the wireless sensor networks through designing a security unit for the head cluster. The security unit considers a switch for each node by using Linear Feedback Shift Registers (LFSR), till each node encode its data with the key and transfer it to the next node. In this algorithm, security coefficient and sensitive tasks are increased for networks with specific activities and the stepwise algorithm is used instead of end to end algorithm to ensure reliability of package arrival to solve the congestion problem. In this algorithm, limitations of sensor networks such as limited energy and small size of nodes buffer are taken into account. Results of the evaluations carried out by NS2 simulator have shown that delay in package arrival is reduced, using such algorithm, fewer energy is consumed by the nodes and network lifetime is increased, accordingly.

Keywords: Wireless sensor networks, transfer layer, congestion control, congestion diagnosis, portability, linear feedback shift registers, security unit

Introduction

Recent developments in the field of electronics and wireless communication have provided the conditions for designing and making sensors with lower power consumption, small sizes and different applications. These small sensors which can operate as various environmental data receiver based on the type of sensor, data processor and transferor, resulted in the advent of an idea to create and develop networks called wireless sensor networks. A sensor network is composed of several sensor nodes which have been spread widely in the environment, collecting needed data from the environment. The location of sensor nodes is not necessarily predetermined. Such characteristic enables us to release them in unavailable and dangerous places. One of the most exclusive features of wireless sensor networks is capability of cooperation and participation among sensor nodes. Each group of sensors has a processor on its board and instead of sending all raw data to database to nodes which are responsible for data processing and conclusion, first we should do some initial and simple processes on the obtained data and then send semi-processed data. Combination of hundreds or thousands of small sensors provides new facilities. In fact, the power of wireless sensor networks relies on the ability to use a lot of small nodes which should be collected and organized and in the various cases such as synchronous routing, managing environmental conditions, managing structures or equipment’s health in the system are also used.

Wireless networks operate using radio signals for data communication. Using such signals, if they crack security barriers of the networks, hackers or unknown nodes can introduce themselves as the network member and have access to critical information, illegally, attack the group and organization's servers, destroy data, cause disruption in the network nodes communication, produce misleading and unreal data, abuse effective bandwidth of the network and other destructive activities.

Moreover congestion has destructive effects on the networks, leading in the limited energy and data loss in the nodes. Hence the congestion should be controlled appropriately. In general, different protocols have been introduced for transfer layer of the networks, each of which is able to control the congestion, effectively. So, security and congestion control are crucial in the networks.

Hence, in this article, a new algorithm has been proposed to increase wireless sensor networks security through designing a security unit for head cluster where permeability of unknown intruder nodes to sensor groups which transfer data to the head cluster, is decreased. The security unit considers a switch for each node by using Linear Feedback Shift Register, till each node encode its data with the switch and transfer it to the neighboring node. This process continues till data reach to the head cluster. Finally the only address of the first node and the precedent node of head cluster is encoded with the data and sent to the head cluster. Using optimal rout table and node specifications table, the head cluster is able to decode the related data to send it to the base station. Moreover, step by step algorithm was used instead of end to end algorithm for congestion control and ensuring reliability guarantee of the package arrival.

In this algorithm, the limitations of sensor networks such as limited energy and smaller size of the node buffer are taken into account.

Implementation of the proposed algorithm increases security coefficient for wireless sensor networks.

In this article first, we will review the related literature and a number of the most important protocols are explained briefly and we will get familiar with head cluster-oriented wireless sensor networks.

Then the transfer layer for the sensor networks will be introduced and we will investigate LFSR and its features. Next sections will proceed on describing the most important responsibilities of transfer layer and different phases of congestion control.

After that the proposed algorithms will be suggested and finally we will proceed on evaluation and conclusion of the study results.

Review of Literature

The protocols proposed for computer networks transfer layer can be divided into two groups:

Group 1: TCP and UDP transfer layer protocols which have been proposed for traditional networks, but are not appropriate for sensor networks.

Group 2: Protocols of this group are proposed for sensor networks transfer layer. Among the proposed protocols, some only control the congestion and some only guarantee reliability and a limited number of these protocols can guarantee both reliability and the congestion.

CODA(2): The aim of this protocol is congestion control in the sensor networks. In this algorithm every node can diagnose the congestion and announce the congestion to other nodes and control its own rate. Details of the protocol are so that every node can detect the congestion based on criteria such as internal queue length, channel position or reduced energy of a message. The detector node sends the congestion to its neighboring nodes. Every node receiving the message, transfers it to the neighbor. When the source received the congestion message, it halves data sending rate. The intermediate node stops sending message when it received congestion message.

STCP: this protocol guarantees both criteria of reliability and congestion control. The protocol is a continuous, measurable and reliable protocol of data transfer, most tasks of which are carried out at the main station. STCP protocol presents an algorithm to control variable reliability, diagnose congestion and prevent congestion. Moreover it supports multiple applications in the network. Reliability of the protocol is guaranteed in the end to end algorithm and congestion diagnosis is carried out by internal queue length of the nodes.

Head Cluster-Oriented Wireless Sensor Networks and Introducing Transfer Layer

The sensor networks are composed of nodes which confront energy limitation. Hence keeping consumed energy in relation to controlling nodes has been proposed in the other articles with multiple arrangements, routing technologies with knowledge about energy amount. Such technologies impose overload. To prevent such overload loss and to consume imbalanced energy, some nodes with much energy called head cluster are placed in the network. These nodes employ a group of sensors in the system to form distinguished cluster and manage them.

Transfer layer protocols, generally, are used for congestion control, packages loss reduction, observation of justice in dedicating bandwidth and providing end to end reliability in the computer networks. Congestion compresses and changes normal data and might result in packages loss. Moreover package loss not only influences reliability but also causes decreased reliability and energy loss. Hence, some protocols are introduced which are special for transfer layer in the wireless sensor networks to control congestion efficiently and guarantee reliability.

Linear Feedback Register Shift (LFSR) and Congestion Control

The constituting components of the feedback register shift depend on the feedback and register shift. Shift register is a number of delay elements arranged next to each other, each having storing capability of 1 b with one input and one output. The length of the register shift is calculated in ratio of bit and includes number of bits which can be placed at the shift register. If a shift resister has n bits it means that n delay elements (n-1, …, 2,1,0) are next to each other. With n bits inside the shift register, just one bit is considered as output at a time unit. Fig (1) shows a scheme of a feedback shift register.

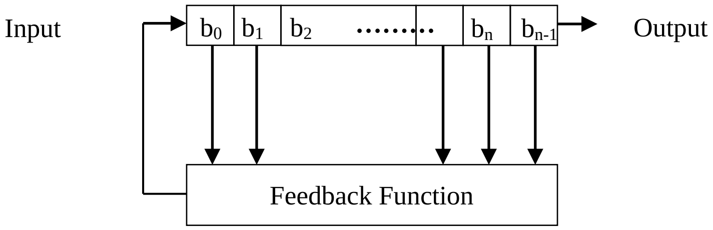

Figure 1: Feedback shift register

Feedback function is a function which acts on specific bits of shift register. It produces n-1 state value. Of course at more simple state, the function is considered as the same XOR. The feedback function can be considered as follows:

Fixed values of Cn-1, …, C1, C0 are feedback coefficients, being considered as switch in a way that if C1-1=1, the switch will be closed, otherwise it will be open.

There are, generally, two main reasons for congestion in the wireless sensor networks. The first reason is that rate of the package arrival is much higher than package service rate. This happens mostly in the nodes which are close to the target nodes, since they carry more combined increasing traffic with themselves. The second reason is related to efficiency aspects at link level such as competition, intervention and bit error rate. The congestion in the wireless sensor networks has direct influence on the energy efficiency and service quality. For example the congestion can result in buffer overload and this causes bigger queue delay and more loss in the packages. Package loss not only causes reduces reliability and service quality but also loses limited energy of the nodes.

Crash in the time of transfer increases package service time and decreases energy. Hence congestion should be controlled in the wireless sensor networks efficiently, avoiding congestion occurrence and congestion decrease. Different congestion control techniques have been proposed for wireless sensor networks. All target congestion control mechanisms have the same foundation. All of them, firstly, attempt to identify and detect congestion, after congestion diagnose, they should inform other nodes about the congestion condition. Generally, there are three phases for congestion control: Congestion detection phase, congestion announcement phase and rate regulation phase.

Proposed algorithms

This unit involves an 8-bit fixed value and a software pseudo-random numbers' generator such as LFSR. The operation way of the system is so that first the controller node gives a switch to the group leader. Such switch endowment to each group leader has several advantages:

-in the case of receiving wrong data it is possible to identify defective cluster and the controlling node should investigate the issue.

- In the case of destruction or problem in a cluster head, it is possible to substitute it with other head cluster

After dedicating switches to the head cluster, each head cluster with proposed security unit for each available group in the cluster dedicates a specific value as identification value.

With dedication of such value to the node, when a node wants to send a data to its head cluster, first it encodes the data with the switch, and then the first group adds its identification number to the data and sends it to the next node. The next node encodes again the data with its related switch and transfers it to the next node after adding related identification number. Firstly, the node checks its precedent node's identification code (identification of the neighbor), then encodes the data, eliminates identification No of precedent node and adds its own identification number. The procedure continues till the encoded data to reach precedent node of the head cluster. The precedent node of the head cluster omits identification number of its neighbor and adds its own number. This continues till the data to be encoded and reach the head cluster. Considering that the specific switch of each group is available with its number in the related table at the head cluster memory unit and also the covered rout from first node to the last node is available at the rout table (12) the first node sends its number along with the data. Hence the head cluster is able to identify the rout covered by the data and decode the encoded data.

Different parameters were used for congestion detection in the congestion control mechanism introduced for the sensor network. In our proposed algorithm the intermediate nodes are responsible for congestion detection. These nodes can detect the congestion using their internal queue length. If the congestion is high, the packages arrival rate to the intermediate notes increases compared to servicing rate at the nodes and the number of the waiting packages in the queue increases to get service.

In this case, the group detecting the congestion enters congestion announcement phase and informs other groups about the congestion. Using such congestion algorithm the congestion is detected rapidly by the intermediate nodes. And implicit method is used to do this. After congestion was detected, each group sends CN bit in the head files of the packages to the target. Moreover it adjusts the CN bit in the NACK packages sent to the source.

Conclusion and Future Studies

Considering the importance of the security in the wireless sensor networks, data transmission among the nodes should be sufficiently safe and reliable. In this article we presented a new algorithm to promote security in the wireless sensor networks through designing a security unit for the head cluster which decreases permeability of unknown intruder nodes to sensor nodes. In this proposed algorithm the data sent among the groups are encoded by LFSR till it needs to be decoded in the case of wiretapping. In these types of encryption, head cluster plays a crucial role in the cluster and data decoding. The default is that rout table is available in the head cluster. In the future studies it would be attempted to set the data among the nodes in a way that the head cluster to be able to decode the data needless of the rout table and switch tables, being aware of precedent node. Moreover the data sent form head cluster to monitor node should be encoded, too.

In the wireless sensor networks the probability of congestion occurrence is high in the nodes due to convergence of data sending toward target node limited size of the buffer. In this article a new congestion control mechanism was developed for sensor networks. Using this algorithm average delay of package arrival is decreased, less energy is lost in the sensor nodes and consequently the lifetime of the network is increased and the congestion occurrence is avoided.

References

Akyildiz, I.F., Vuran, M.C., Akan, O.B., & Su, W. (2010). Wireless Sensor Networks: A Survey. Department of Electrical and Electronics Engineering Middle East Technical University, Ankara, Turkey.

Chan, H., Perrig, A., & Song, D. (2013). Random key predistribution schemes for sensor networks. In IEEE Symposium on Research in Security and Privacy.

Eschenauer, L., & Gligor, V.D. (2012). A key management scheme for distributed sensor networks", In Proceedings of the 9th ACM Conference on Computer and Communication Security, pp. 41-47, November 2012.

Gupta, G., & Younis, M. (2011). Fault -Tolerant Clustering of Wireless Sensor Networks. IEEE, pp.1579-1584.

Hull, B., Jamieson, K., & Balakrishnan, H. (2011). Mitigation congestion in wireless sensor networks. In proceeding of ACM symposium, USA.

Iyer, Y.G., Gandham, S., & Venkatesan, S. (2011). STCP: A generic transport layer protocol for wireless sensor networks. In Proc. International Conference on Computer Communications and Networks (ICCCN) Houston ,pp.449-454.

Sengottaiyan, N., & Somasundaram, R. (2010). A Modified Routing Algorithm for Reducing Congestion in Wireless Sensor Networks. European Journal of Scientific Research , 35 (4), 529-536.

Singh, S., Woo, M., & Raghavendra, C.S. (2013). Power-Aware Routing in Mobile Ad Hoc Networks, Proceedings of ACM MOBICOM'98, Dallas, Texas, October 2013.

Wan, C.Y., Eisenman, S.B., & Campbell, A.T. (2013). CODA: Congestion detection and avoidance in sensor networks. In Proc. of the First International Conference on Embedded Networked Sensor Systems (Sensys), Los Angeles, pp.266-279.