International Journal of Current Engineering and Technology
ISSN 2277 - 4106

Available at http://inpressco.com/category/ijcet

Research Article

Energy Efficient and a Secure Heterogeneous Wireless Sensor Networks Using Scheduling and Intrusion Detection

Geethu K T[a*] and Archana J N[a]

[a]Atria Institute of Technology Affiliated to VTU Belgaum Karnataka

Accepted 26 July 2013, Available online 01 August 2013, **Vol.3, No.3 (August 2013)**

Abstract

Nowadays the use of wireless sensor networks is a common activity. For this reason there are many works trying to solve the main inconveniences of the wireless sensor networks the energy consumption and security. Traditionally, these networks were composed only by sensors, but now routers have been included in order to facilitate communication among sensors and reduce energy consumption at the same time. A Heterogeneous Wireless Sensor Network consists of many sensor nodes, routers and a base station. The number and type of sensor nodes and the design protocols is application specific. The sensor data in this application may be light intensity, temperature, pressure, humidity and their variations. Scheduling and Intrusion Detection are the two areas which are given more attention in this paper. In this paper, we propose a new approach of an Intrusion Detection Based Security Solution and Sleep /Wakeup Scheduling protocol for Wireless Sensor Networks.

Keywords: *Heterogeneous Wireless Sensor Networks, Scheduling, Intrusion Detection System, Medium Access Control.*

1. Introduction

The use of wireless sensor networks has increased substantially in the last years. Both, boom of this technology and its versatility have favoured the appearance of applications in civil areas (industrial control, environmental monitoring, intensive agriculture, fire protection systems, and so) and military areas (rescue operations, surveillance, etc.).

As the wireless Sensor Networks are made up of tiny energy hungry sensor nodes, it is a challenging process to retain the energy level of those nodes for a long period. They are equipped with limited computing and radio communication capabilities. This work is on the attempt to reduce the power consumption of nodes, by concentrating on the radio, which has four states of operations at various time intervals. Wireless Sensor Networks are made up of tiny sensors which are used for monitoring or sensing data. Because of their small size, power supply is provided by a small battery, which, when deployed in a 'not-easily reachable' place, cannot be replaced or recharged frequently. The purpose of all these nodes is to monitor the required data and send them to a Base station which may be in a remote place.

Storage mechanism is also very simple and can only provide limited space. So acquisition of precise data and immediate transfer of the data to sink node is very important. Data processing and data transfer require more power. When, the data has to be transferred and when, it needs to be stored depends on the state of the radio in the node. To conserve Energy, we can switch the radio to sleep state when there is no data to send or receive. This method of making the radio to be in sleep state and making it active if any event is detected is called as on-demand scheme or event-based scheme.

There is another method of scheduling i.e. on regular time interval all the nodes will be either in sleep mode or active mode. This is synchronous scheme. But the overhead of maintaining all the nodes in the synchronized state becomes complex. It is not necessary to keep all the nodes active at one time. WSN can follow a scheduling pattern, accordingly, at any instant; we can make only a limited number of nodes active. The work presented in this paper is based on this type of asynchronous mechanism.

Security is becoming a major concern for protocol designers of WSN because of the broad security-critical applications of wireless sensor networks (WSNs). To protect a network, there are usually several security requirements, which should be considered in the design of a security protocol, including confidentiality, integrity, and authenticity. An effective security protocol should provide services to meet these requirements. In many cases, no matter how carefully we design a security infrastructure for a network, attackers may still find a way to break into it and launch attacks from the inside of the

*Corresponding author Geethu K T is a M.Tech student and Archana J N is working as Asst. Prof

network. If they just keep quiet to eavesdrop on traffic flows, they can stay safe without being detected. If they behave more actively to disrupt the network communications, there will be some anomalies, indicating the existence of malicious intrusion or attacks. An intrusion can be defined as a set of actions that can lead to an unauthorized access or alteration of the wireless network system. Intrusion detection mechanisms can detect malicious intruders based on those anomalies. Intrusion detection system (IDS) attempts to monitor computer networks and systems, detecting possible intrusions in the network, and alerting users after intrusions had been detected, reconfiguring the network if this is possible. Usually, the neighbours of a malicious node are the first entities learning those abnormal behaviours. Therefore, it is convenient to let each node monitor its neighbours such that intrusion detection mechanisms can be triggered as soon as possible.

In this paper, we propose a new approach of an Intrusion Detection Based Security Solution for Heterogeneous Wireless Sensor Networks. In the proposed methodology, an efficient MAC address based intruder tracking system has been developed for early intruder detection and its prevention.

The paper is organized as follows. Section 2 describes design of heterogeneous wireless sensor networks. Section 3 describes the scheduling mechanism. Section 4 provides summary of security requirements for WSN. Section 5 describes the security solution for WSN. Section 6 is about Simulation and Conclusion is given in Section 7.

2. Heterogeneous wireless sensor networks

Most of the protocols designed for WSNs assume that the sensors have the same capabilities in terms of storage, processing, sensing and communication. The resulting network is said to be homogeneous. In these types of networks, a pair of sensors would have the same lifetime if they have the same energy consumption rate. Some sensing applications, however, use sensors with different capabilities and accordingly the resulting network is said to be heterogeneous. In the real world, the assumption of homogeneous sensors may not be practical because sensing applications may require heterogeneous sensors in terms of their sensing and communication capabilities in order to enhance network reliability and extend network lifetime Also, even if the sensors are equipped with identical hardware, they may not always have the same communication and sensing models. In fact, at the manufacturing stage, there is no guarantee that two sensors using the same platform have exactly the same physical properties. This taxonomy focuses on heterogeneity at the designing stage, when sensors are designed to have non identical capabilities to meet the specific needs of sensing applications.

Cluster-based approach is developed for WSNs. In this approach, a network is divided into clusters. Each cluster head monitors its cluster members. All the members in a cluster are further divided into groups and the groups take turns to monitor the cluster head. Since routers have also been introduced, these routers act as cluster heads. Not all the sensor nodes keep monitoring, thus reducing the overall network energy cost.

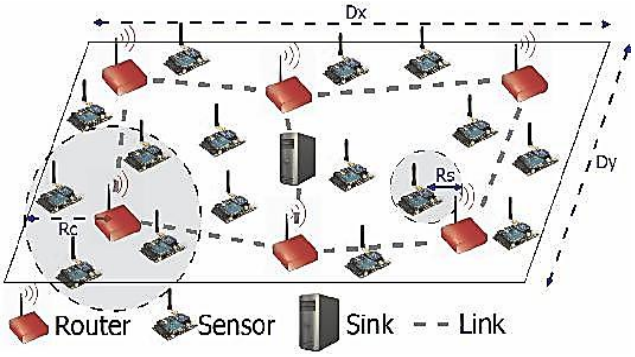


Figure 1 Heterogeneous Wireless Sensor Networks

3. Scheduling

As a sensor node in WSN is small, its power supply unit should be very small and also it should support all its operations without degrading the performance. The communication protocol used should be light weight and it should not consume more energy. Hence, we are going for a good scheduling protocol and while applying it, power consumption is the one which should be kept in mind.

Any Scheduling protocol will keep only a subset of nodes to be in active state and keeping others in-active or in sleep state. A scheduling protocol will be the best if it keeps only a minimum number of nodes active at any instant. There are so many scheduling protocols available. For a WSN, a scheduling protocol should use narrow band modulation techniques. Low data transfer rate is enough for a WSN in Environmental monitoring applications.

The TDMA (Time Division Multiple Access) based scheduling protocols make the nodes to be in inactive mode, until their allocated time slots. The TDMA based protocols [8] are designed such that the shortest path for communication will be found out and only a particular link will be in wake up mode for a transmission.

Any scheduling protocol for the WSN for Medium Access Control (MAC) should have the following:

- Narrowband Modulation techniques.
- Good throughput efficiency.
- Moderately low Data transfer rate.
- Less Hardware complexity.
- Low access delay, low transmission delay and low overhead.

The TDMA based scheduling allocates separate time slot for each node to access the medium to send the sensed data or to forward the aggregated data.

A. Sleep/Wake-up Scheduling

For an asynchronous type of sleep/wake-up scheduling periodically only certain nodes have to wake-up and send

or receive. All the other nodes should be in sleep state. While going for a switch from active to sleep state, and then from sleep to active state, the condition to be checked is that the energy it consumes for the switch should be low when compared with the energy it consumes when it is always in the active state.

Ewasted in switching < Esaved

This scheduling protocol is designed based on the radio of the node
r-Radio in sleep state
rs-Radio in transmitting state
rt-Radio in receiving state rrl-Radio in listening state

The energy consumed for the switch can be represented by Esl(sleep to listen), Est(sleep to transmit) and Esr(sleep to receive). For a time slot, say 't', if the node is in sending state, it will be denoted by rt,t=1. If it is not in sending state, it will be denoted by rt,t=0. So at a particular instant say t, a node can be in any one of the four states. So we can state the condition like this

rt,t+ rr,t+ rl,t+ r s,t=1

For the state switch from sleep state to listening state, the energy consumed can be calculated by t (rs,t+ rl,t+1) Esl.
During every cycle, the radio goes to all the four states. When the radio is either sending or receiving or simply listening, it is said to be active. If it goes to sleep, it is said to be in sleep state.
The Energy wasted in simply switching between states
Ewasted in switching can be calculated by

Ewasted in switching= ts-a(pactive+ psleep)/2

During every cycle, the radio goes to all the four states. When the radio is either sending or receiving or simply listening, it is said to be active. If it goes to sleep, it is said to be in sleep state.

The Energy saved because of this switching can be calculated by

Esaved = (ta-ts) pactive – (ta-s (pactive + psleep)/2) + (ta-ts-ta-s) psleep

In this work, the basic scheduling is designed based on this first check i.e.

Ewasted in switching < Esaved

4. Security requirements for WSN

Security for wireless sensor networks should focus on the protection of the data itself and the network connections between the nodes [9]–[12]. In general, security requirements often vary with application. In WSNs we can distinguish the following important requirements of security capabilities: authentication and authorization, availability, confidentiality, integrity and freshness. Thus, we need some mechanism for access authorization and protecting a mobile code. In many applications we need to protect fair access to communication channels and at the same time we often need to hide the information about physical location of our sensor node. Moreover, we need to secure routing and we have to defend our network against denial of service, malicious flows, node capturing and node injection, etc.

Table 1 Notation used

Notations	Descriptions
r_s	Radio in sleep state
r_t	Radio in transmitting state
r_r	Radio in receiving state
r_l	Radio in listening state
E_{sl}	Energy consumption during the switch from sleep state to listen state
E_{st}	Energy consumption during the switch from sleep state to transmitting state
E_{sr}	Energy consumption during the switch from sleep state to receiving state
p_{active}	Power consumed in active state(r_t,r_r,r_l)
p_{sleep}	Power consumed in sleep state r_s.
t_{s-a}	Time taken for going to active state(r_t,r_r,r_l) from sleep state.
t_{s-a}	Time taken for going to sleep state from active state(r_t,r_r,r_l).
t_a	Time at which the radio becomes active as per the schedule to send or receive any data.
t_s	Time at which the radio decides to go to sleep state as per the schedule.

Authorization. Data authorization specifies acess rights to resources and is strongly related to access control. Access control should prevent unauthorized users from participating in network resources. Hence, only authorized users can join a given network. Access control relies on access policies that are formalized, like access control rules in a computer system. Most modern operating systems include access control.
Authentication: As in conventional systems, authentication techniques verify the identity of the participants in a communication, distinguishing in this way legitimate users from intruders. In the case of sensor networks, it is essential for each sensor node and base station to have the ability to verify that the data received was really send by a trusted sender and not by an adversary that tricked legitimate nodes into accepting false data. If such a case happens and false data are supplied into the network, then the behaviour of the network could not be predicted and most of times will not outcome as expected.
Availability: Availability ensures that services and information can be accessed at the time that they are required. In WSNs there are many risks that could result in

loss of availability such as sensor node capturing and denial of service attacks. Lack of availability may affect the operation of many critical real time applications. Therefore, it is critical to ensure resilience to attacks targeting the availability of the system and find ways to fill in the gap created by the capturing or disablement of a specific node by assigning its duties to some other nodes in the network. If a node serves as an intermediary or collection and aggregation point, what happens if the node stops functioning? The protocols employed by the WSN need to be robust enough mitigate the effects of outages by providing alternate routes.

Confidentiality: Confidentiality requirement is needed to ensure that sensitive information is well protected and not revealed to unauthorized third parties. The confidentiality objective is required in sensors' environment to protect information traveling between the sensor nodes of the network or between the sensors and the base station from disclosure, since an adversary having the appropriate equipment may eavesdrop on the communication. By eavesdropping, the adversary could overhear critical information such as sensing data and routing information. Based on the sensitivity of the data stolen, an adversary may cause severe damage since he can use the sensing data for many illegal purposes, e.g. sabotaging, blackmail. Furthermore, by stealing routing information the adversary could introduce his own malicious nodes into the network in an attempt to overhear the entire communication. If considering eavesdropping to be a network level threat, then a local level threat could be a compromised node that an adversary has in his possession. Compromised nodes are a big threat to confidentiality objective since the adversary could steal critical data stored on nodes such as cryptographic keys that are used to encrypt the communication.

Integrity: Moving on to the integrity objective, there is the danger that information could be altered when exchanged over insecure networks. Lack of integrity could result in many problems since the consequences of using inaccurate information could be disastrous. Integrity controls must be implemented to ensure that information will not be altered in any unexpected way. Many sensor applications such as environment and healthcare monitoring rely on the integrity of the information to function with accurate outcomes. Therefore, there is urgent need to make sure that information is traveling from one end to the other without being intercepted and modified in the process.

5. Proposed intrusion detection based security solution

The emphasis of our approach is to detect and prevent the intruder in the sensor network by implementing MAC address based intruder tracking system.

Basic assumption:

- The Base Station (BS) is located far from the sensors and immobile.
- The BS has the information about the location of each node.
- Assume 100 nodes in the network.

Function of Base Station:

- All nodes are able to send data to BS via Router.
- Base station has all the information regarding each Cluster (number and MAC addresses)
- The removal or addition of any node in a Cluster is monitored by the Base Station.
- Poll status of each node is received with MAC address.
- Base station runs task of MAC address tracking, MAC address history and management of databse.
- The Base Station has the capability to seize the operation of any node in the network.

Function of Router:

- Router keeps track of each node and sends periodic status information to the Base Station.
- Router receives data from its nodes and sends necessary information to Base Station.
- Router transmits data to Base Station after performing data reception and compression.

A. Layout of the Wireless Senor Network

As shown in Fig. 1, let us assume a wireless sensor network consisting of 10 Routers (R1 to R10) with their node forming the clusters. Nodes send data to their respective Routers within each cluster. As shown in Fig. 2, the Router collects data from each node, compresses the data and transmits it to the Base Station (BS). Routers keep track of each node and send periodic status information to the BS.

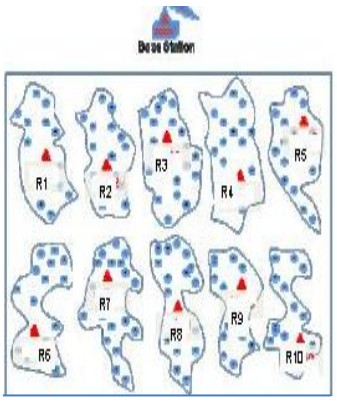


Fig. 1 Layout of WSN

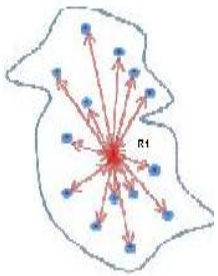


Fig. 2 Data communication between nodes and R1

Flow chart at next page illustrates the logic of the proposed intrusion detection based security solutions for heterogeneous wireless sensor networks.

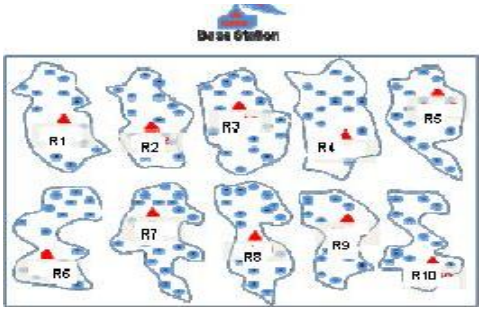


Fig. 3 Data communication between Routers and BS

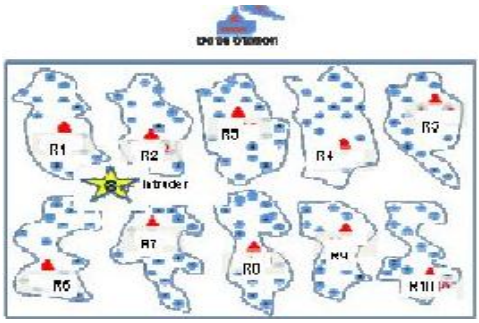
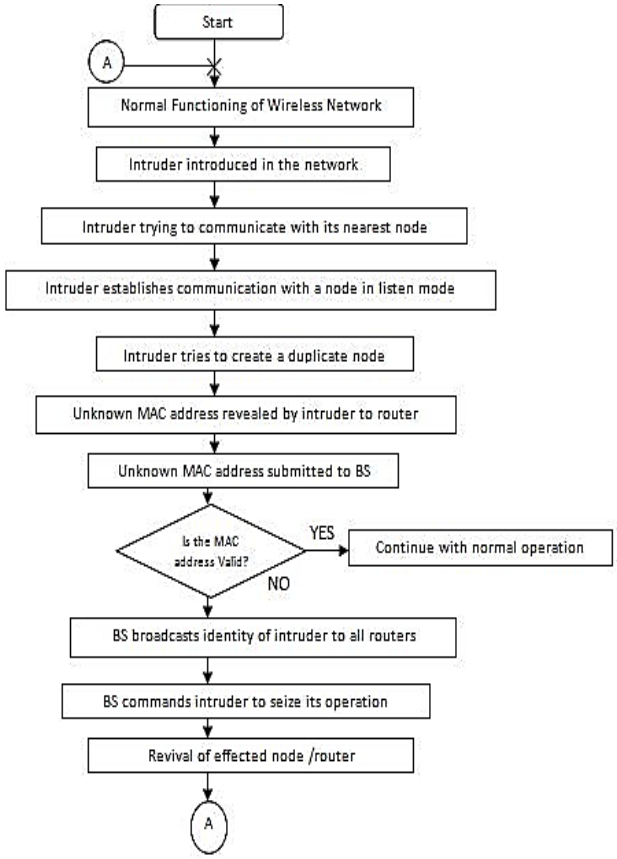


Fig. 4 Intruder introduced in the network.



6. Simulation

The sleep/wake-up scheduling is tested in a simulated WSN and prove that it provides energy efficient Heterogeneous Wireless Sensor Networks. A graph between Power Consumption and No of nodes is plotted to prove that the system consumes negligible additional power for implementing intrusion detection based security solution and also it is very energy-efficient.

Conclusion

The proposed algorithm in this paper is completely TDMA based. It helps to reduce the energy consumption by reducing the number of times; a node has to wake up, during a time slot, to be in active mode. Effort is put to prove that the underlying concept in this paper is efficient usage of energy. The future work can be done by combining both the TDMA and FDMA based slot allocation.

We have also illustrated MAC address based intruder tracking system for heterogeneous wireless sensor networks. This proposed system implements base station based detection and thus is very energy-efficient for early detection and prevention of security threats and attacks. Early detection and prevention of the intruder by efficient security system can prevent many problems like slowing down of the network, sending of fake data, etc. By designing a security system in which the Base Station (BS) keeps track of the security of the Wireless network, high security can be ensured without any significant energy overheads on individual nodes and routers.

References

GI. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci (2002), A survey on sensor networks, *IEEE Communications Magazine*,102–114.

Vieira, M.A.M, Coelho, C.N, Jr. da Silva, D.C. (2003) Survey on wireless sensor network devices. Emerging,*Technologies and Factory Automation, 2003. Proceedings.* ETFA '03. IEEE Conference

Pottie GJ, Kaiser WJ (2000) Wireless integrated network sensors.*Commun ACM* 43(5):51–58.

Yick J, Mukherjee B, Ghosal D (2008) Wireless sensor network survey. *Computer Netw* 52(12): 2292– 2330.

Jun Zheng and Abbas Jamalipour (2009), Wireless Sensor Networks: A Networking Perspective, a book published by *A John & Sons, Inc, and IEEEE.*

R. Bace (2000), Intrusion Detection, *MacMillan Technical Publishing*.

Dilip Kumar and R.B Patel (Jumy 2010), Prolonging network lifetime and data accumulation in heterogeneous sensor network *International Arab Journal of Information Technology* Vol.7,No.3

Christophe J. Merlin, Wendi B. Heinzelman (2009), Schedule Adaptation of Low-Power-Listening Protocols for Wireless Sensor Networks, *IEEE Transactions on Mobile Computing*, vol. 9, no. 5, pp. 672-685, May 2010 doi:10.1109/TMC.2009.153.

M. Ahmad, M. Habib, and J. Muhammad (2011), Analysis of security protocols for Wireless Sensor Networks, in *Proc. 3rd Int. Conf. Comp. Res. Develop. ICCRD* , Shanghai, China, 2011, vol. 2, pp. 383–387.

C. Castelluccia, A. C.-F. Chan, E. Mykletun, and G. Tsudik (2009), Efficient and provably secure aggregation of encrypted data in wireless sensor networks, *J. ACM Trans. Sensor Netw*. (TOSN), vol. 5, no.3.

S. R. Gandham, M. Dawande, R. Prakash, and S. Venkatesan, S. (2003), Energy efficient schemes for wireless sensor networks with multiple mobile base stations, in Proc. *IEEE Global Telecom. Conf. GLOBE- COM'03, San Francisco,* USA, vol. 1, pp. 377–381.

J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary (2007), Wireless sensor network security: a survey, in Security in Distributed Grid, Mo- bile and Pervasive Computing, *Y. Xiao, Ed. Auerbach Publication*.