ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

WIRELESS SENSOR NETWORK, VARIOUS ISSUES AND NEED OF SECURITY- A REVIEW

Rajesh Ku. Chakrawarti*, Anurag Punde
Department of Computer Science,
Shri Vaishnav Institute of Technology & Science, Indore-452001

ABSTRACT

This new Modern era is full of various new and promising technologies which are capable enough to change the entire world within the fraction of a second. Wireless Sensor Network is the one which is going to play the vital part in this modern scenario. This particular technology shows some great promising feature for the various sector like military as well as public. Combined with various other technology it can be sufficient to solve many problems arising day by day. But like all the other technology it lacks in some fields. In this paper we will try to review this technology as well as issues and security requirements.

KEYWORDS: Attack, Autonomous sensor, Power, Security Sensor, Wireless Sensor Networks (WSN).

INTRODUCTION

Various technologies are influencing our day to day life including the wireless sensor networks. Wireless sensor networks first handedly designed for the military purpose only. Their main work was to do the surveillance work in the battle field. After many years of that discovery the industrial use of these had started [1]. Now a days this technology has become so powerful that it is used in so many of the area like patient monitoring, environmental studies, and home or office automation etc... Sensor nodes are generally those systems which are automated, self organizable, having sensory perception for various elementals, some sort of energy generator like battery, a particular transmission media. When these were used in early days thy have a size of like a shoebox but later they became very tiny. The biggest of the deployment of these came into the market in the 21st century where these are used as latest smart phones [2]. The term wireless is something refer to a particular system which is wire free. Simply means that these system have RF generator or some sort of signal generator with transceiver to transfer and reception of data. Combining these two major components form the ultimate technology named wireless sensor networks. The diagram is given below for the basic understanding of the system architecture:-

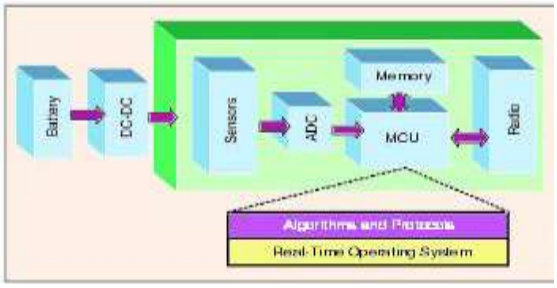


Figure 1. System architecture of a typical wireless sensor node

The generally proposed ideas for the sensor node system architecture is SINA (sensor information networking architecture) which is also called the middle ware architecture. Generally sensor nodes are very energy driven nodes they consume lot of energy due to their transmission capabilities over wireless network. These system run on the battery power which is bound to be depleted in due time [3]. The sensor life is very depend on it. If it runs out over use sensor will stop working if it is not rechargeable. This is the main issue with these systems which is discussed in later part. Each and every unit is fully functional under the consideration of the battery use. Mainly have four sub-systems:-

I. **Computing Sub-system:** generally consist of a Microprocessor called MCU mainly responsible to control the sensor and also the working of communication protocols deployed. MCU operates in different modes which usually require lot of power consumption while switching from one node to another hence the battery or power source must be picked considering the same.

II. **Communication Sub-system:** this is a high power consumption unit. It consist of a radio unit working in a short range. This unit is responsible for the communication with the neighbor nodes and the world outside. It operates in 4 different modes like transmission, receiver, idle and sleep. It is suggested to put this unit totally off rather than in idle mode considering the high power consumption.

III. **Sensor Sub-system:** this unit is consisting of sensor and actuators group with a link to the outside world. The energy consumption is depend on the power components. It is advised to use low power components and power saving when not in use.

IV. **Power Supply Sub-system:** this unit consists of a power source, typically a battery. Which is responsible for the power supply for the entire working of the system [4]. Usually high power consumption occur that can cause battery power depletion though it could have last longer. Battery life can be increased by reducing the current supplied to the system drastically or just by turning it off when not in use.

We can reduce the total power consumption just by design the system as energy efficient which will automatically increase the total life of the system. These wireless sensor node also work as a router which are responsible to transmit the data packets from one node to another over the network. Since these sensor networks are placed over various geographical locations it takes lot of computing power for the communication and the transmission of the data packets regardless of the route we choose is the same [5]. The operating system is responsible for the entire working of the system it is mandatory that it should be energy aware so the system can be used for the longer period of time while conserving the power. Which can make the communication more difficult as the transmission to the next node will take lot of time and energy. Using the beacon is the nice option for this problem while once set the node can become the beacon for other nodes to communicate.

LITERATURE REVIEW

Kheyali Mitra, Urban Computing and Information Management System Using Mobile Phones in Wireless Sensor Network, March 2010: in the today's scenario mobile phones are becoming the need of every user rather than the Pcs. With the help of which, we are managing all the information on wireless sensor network. Mobile phone will be the main access point in Wireless Sensor Network [11]. The system will be as simple as possible providing all the facilities those are available in web based rather PC based applications regarding this. The user has two choices using which he/she can get the required information namely (i) get the reports regarding all/individual tags and or routes, emergency messages, sensors and also the location information; (ii) send command to the server using which immediate decision about the system can be taken from server side. The user can see the report in their phone's display screen. These will make the whole process more users friendly. This system provides the same facilities those are available in common web based rather PC based applications. It is easy to use and simple to handle.

Sophia Kaplantzis, Security Models for Wireless Sensor Networks, March 2006: Wireless Sensor Networks (WSNs) are a new technology foreseen to be used increasingly in the near future due to their data acquisition and data processing abilities. Security for WSNs is an area that needs to be considered in order to protect the functionality of these networks, the data they convey and the location of their members. The security models & protocols used in wired and other networks are not suited to WSNs because of their severe resource constrictions [12]. In this report we highlight the research to date in the area of security for WSNs and propose a solution based on intrusion detection systems and efficient classifiers. The idea is to generate a security model that will provide energy efficiency and fault tolerance to WSNs under attack. In this report we introduced the technology of WSNs. In some sense we highlighted possible WSN applications, their network architecture, their hardware specifications and their security vulnerabilities. Much research has been done on the topics of secure routing and wireless encryption. However, simplifying IDSs for such applications is an area yet to be fully investigated. In this paper the author proposed the development of a fault tolerant and energy efficient intrusion detection model that will enhance the lifetime of a network under attack, by incorporating state of the fast classifiers and mathematical strategies. The author in this paper also focuses upon the hardware to improve the performance and conclusion.

E. Ladis, Secure, and Mobile Visual Sensor Networks Architecture, 2009: As Wireless Sensor Network–based solutions are booming they are facing new encounters: they must be capable of adapting to rapidly changing

environments and requirements while their nodes should have low power consumption as they usually run on batteries [13]. In this paper the author has discussed the issue like security, cost, the limited bandwidth problem.

Filippe C. Jabour, Mobility support for wireless sensor networks, 2007: In this work, the author proposes a two-tier approach for mobility support in wireless sensor networks. It is based on local interactions among sensors, on global tasks of mobile agents and on location prediction. We demonstrate the correctness of a simple location prediction model. The author also propose, evaluate and compare two algorithms for mobile agents' decision. The proposed scheme is stateless and does not need a routing protocol. All computing (location prediction and mobile agent's decision) are of linear complexity [14]. They have observed a better performance as mobility degree and node density grows. Since there are few proposals to treat general mobility in WSN, we consider this work a promising approach. They have applied simple prediction is to provide location model of constant complexity is suitable for the scarce resources of WSNs and the predictions are sufficient for the decision process of

Al-Sakib Khan Pathan, Security in Wireless Sensor Networks: Issues and Challenges, Feb 2006: Wireless Sensor Network (WSN) is an emerging technology that shows great promise for various futuristic applications both for mass public and military [1]. The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance in future. The inclusion of wireless communication technology also incurs various types of security threats. The intent of this paper is to investigate the security related issues and challenges in wireless sensor networks. The author identify the security threats, review proposed security mechanisms for wireless sensor networks. The author also discuss the holistic view of security for ensuring layered and robust security in wireless sensor networks. Many of today's proposed security schemes are based on specific network models.

ISSUES

The wireless sensor network is a powerful technology which is widely used now a days as its application is seemed limitless as the areas is unbound. Today even the smart phones are acting as WSN which can be used approximately anywhere around the globe. But like any other technology this one also having some flaws. One of which is indicated in earlier discussion. More specific there are some known issues with this technology which should be kept in mind while implementing wireless sensor network for some specific purpose. These various issues with this technology discussed below:

I. Signal Fading

Wireless sensor networks can be placed over any geographical location which may or may not be good for the communication purpose as these locations can be separated from each other under various circumstances the communication media can become very unreliable[4][5]. Sensor nodes generally have limited bandwidth and more limited power supply. Hence the transmission of a signal under such condition can became problem. Not only this but the signal can be weak, tempered due to various obstacles, deflection, reflection, scattering of signal as it can take any direction to reach the targeted node or machine. This whole thing will become worse if the climate is considered to be untrustworthy. In such a way when a signal reach to the target node it can be so weak and distorted that is will become mostly useless as the data will be unprocessable. Hence completely rejecting it make the whole transmission fruitless.

II. Mobility, Size and Cost

Unlike the other wired technologies these systems are not immovable objects. The very basic is that the object can come and go into the range and network for a short period of time just like a user or an autonomous node or system which come and go in the network for short period of time, it changes the network rapidly from one to another because of its movements places to places. Because of this it is very cunning requirement that these sensors should have the mobility so they can also move according to the requirements especially when the handoff occurs because the data packets lost during this transaction [6]. A particular routing protocol is required to handle such condition is mandatory. As the mobility concern the size of these should be very fair enough to support the quick movements. As it is the basic requirements of the establishment of the sensor devices that they should be small enough so they can be movable and can be fit in any geographical location. Considering their use in the military purpose in the beginning they were bigger in size after a short period of time their size cuts in half and now became the one-third of the original size so they can be implemented approximately anywhere around the globe. The cost of these system is yet very high. Even the technologically we have advanced so much but the fact to the matter is the establishment of these systems is very expensive. Depending upon the numbers and usage requirements the cost varies.

III. Power Consumption

These systems usually connected by a power source such as battery which may not be rechargeable as this is a big issue and challenge to the researchers for making a system for the recharging of the battery using some sort of low

cost establishment. As these systems are used continuously over time for the transmission and receiving of the data from one to another while processing the packets for forwarding on any of the chosen route takes lot of battery power [10]. These node generally works on RF (radio frequency) as the transmission medium and can be at any geological places, the transmission can take lot of battery power, even when it is not doing anything it is put into idle mode which also use some of its battery life. Due to all of these the battery power can soon be die out and the whole system or sensor node will become useless. Quite frankly we should consider this particular option while dealing with such systems and the new option for the power source should be explored so that the systems can go on with the working for the longer time.

IV. Data Rate

Controlling and increment of the current data rates is highly essential. As data rate consists of various factors like compression, power control, interference mitigation and the transfer protocols. The transfer of the data at higher rate is the most cunning requirement in today's scenario and the future use. For this purpose we should consider some new and intelligent data transfer protocols that can be used with the understanding of the traffic condition of the network to achieve higher data rates.

NEED FOR SECURITY

Like all the other security is the basic concern of this technology. This is an important issue which should be dealt with. The basic idea to consider this is that there are two different types of attacks which came into play the first one is against the security mechanism of the system while the other one is concern with the basic mechanism like the routing. The following are the most common attacks that should be taken care off.

I. DoS (Denial of Service) Attack

Usually this type of attack initialized by the failure of a node or just the misbehavior of the node. Normally this can be achieved by overwhelming the targeted node with so much useless and unnecessary data packets so that node will become unresponsive or become exhausted to misbehave. Because of this the user using this network won't be able to access any legitimate data or any of the resource thus preventing them and stopping] them in their tracks temporary or completely [1] [7]. This particular attack not only used to disrupt, subvert or destroy the network but also to paralyze the network capabilities to provide any services to the users. DoS attacks can be performed at the various levels of the various layers in wireless sensor networks like in the physical layer it can perform Jamming and Tempering while in the data link it can be collision, exhaustion, at network layer this can be misdirection, Black holes while in transport layer malicious flooding and no other than de-synchronization.

II. During transmitting information

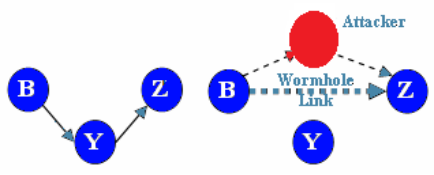
Since we all know that the wireless sensor network is an unreliable medium of transmission which makes it unsecure also. Any third user can easily interfere in an ongoing communication between the two nodes. Suppose there are two sensor node set up in a short range distance transferring the data to each other, since it's not a secure communication as no such mechanism specialty is provided to the nodes or to the network any third user having higher processing power and strong signal range can interfere form long range. By this attacker can perform any of the task like altering the data, stealing of valuable information or even destroy the whole the data in the transit.

III. Black Hole (Sink) Attack

In this type of critical attack the malicious node try to pretend as the base node and attract all traffic in the network especially where the flooding protocol id deployed. It generates a signal convincing all the other nodes that he have the shortest path to the other nodes [8] [9]. Once successfully inserted between the nodes that are communicating each other it can perform any intentional damage to the data packets. By inserting itself and perform any attack it can affect any nodes even if they are far away from the original Base station.

IV. Worm Hole Attack

This is another type of critical attack. Actually this attack have its special significance in wireless sensor network. This attack can be initialized even when the first time a node is inserted into a network and it starts discovering its neighbours, which makes this attack so violent. In this usually an attacker record the data packets and then by using some sort of tunneling it transfer the data packets to the target. The whole transmission tunneling of bits can be done by random selection of bits.



(i) *(ii)*

Figure 3: Wormhole Attack

As we can see in the figure (i) and (ii) above where a wormhole condition is shown. In this example a node B which can be any of the base station or just a sensor node broadcasting a packet for the routing packet containing a request. Attacker listen to this request packet and make a fool out of node B by just simply pretending that the node is in its neighborhood. Now each of the neighbor node will consider this as a token and imagine that it is in the range of node B and then can transmit the packets to it easily and mark this node as their parent node. In this way the attacker make them believe that the intended node is just a single hop away which can be actually very far away from them, thus by creating a Wormhole.

RESULT AND DISCUSSION

Most of the issues are the timely matter as the new research frontiers are working in this area. If we just take care of the power related problem that will be able to solve half of the problems. As new research ideas are implemented in this area this technology will become soon the most reliable and trustworthy of all. The particular security mechanism is yet to be founded because we have to implement the security at each and every level and layer of the network. As we can see that security is a major challenge like the other technologies but I this we do not have any concrete foundation of any particular security protocol which can dealt with all the attack related problems. As promising this technology is, with all the limitless or boundless the possibility of its use we must first consider the limitation which should be dealt with soon enough. As this technology is still is growing there are many issues that are still to be discovered. As this is the emerging field and a partially explored territory, we can see that there are many more application area which are in line with the existing systems. All the previous technologies are sophisticated to some point with the field they were deployed but when we took out the dependency with the area or field it yield the result catastrophic while on the other hand we can see that wireless sensor networks are not only location independent but also the free of any kind of platform dependency. By analyzing about this technology we found that this is not available easily as it is not as cheap as it should be, because of the installation requires lot of setup to be done and it also have the low battery life while security is out of question. The more we analyze this technology we came to the point that after dealing with the small related issues this technology will emerge as the milestone for the upcoming decades in this research field.

CONCLUSION

Wireless sensor network is no doubt an emerging field but its full extent is yet to be discovered. We will be able to deal with basic problems which are directly related to its basic mechanism as more and more researchers are getting interested in this field. Many security problems can be easily rectified by choosing a proper technology or procedure to analyze these problems. Wireless sensor network has wide area of application where they can not only use for military purpose but can serve any organization or even an end user. This technology can be implemented geographically approximately anywhere to analyze the data or even sending the data back to the destination.

REFERENCES

1. Pathan, A.S.K., Hyung-Woo Lee, Choong Seon Hong, " Security in Wireless Sensor Networks: Issues sand Challenges" Advanced Communication Technology, IEEE International Conference ICACT . , 6pp-1048, Feb 2006.
2. Akyildiz, I.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E. "A survey on sensor networks". IEEE Commun. Mag. 2002, 40, 102–114.
3. Tubaishat, M.; Madria, S. "Sensor networks: an overview". IEEE Potentials 2003, 22, 20–30.
4. Hac, A. "Wireless Sensor Network Designs". John Wiley & Sons Ltd: Etobicoke, Ontario, Canada, 2003

5. Raghavendra, C.; Sivalingam, K.; Znati, T. “Wireless Sensor Networks”. Springer: New York, NY, USA, 2004.
6. Culler, D.; Estrin, D.; Srivastava, M. “Overview of sensor networks”. IEEE Comput. 2004, 37, 41–49.
7. Verdone, R. “Wireless Sensor Networks”. In Proceedings of the 5th European Conference, Bologna, Italy, 2008.
8. Chiara Buratti, “An Overview onWireless Sensor Networks Technology and Evolution”, 2009
9. Culler, D. E and Hong, W., “Wireless Sensor Networks”, Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33
10. John A. Stankovic, “Wireless Sensor Network”, published in the year June 19, 2006.Kheyali Mitra, “Urban Computing and Information Management System Using Mobile Phones in Wireless Sensor Network”, March 2010
11. Sophia Kaplantzis, “Security Models for Wireless Sensor Networks”, March 2006.
12. E. Ladis, “Secure, Mobile Visual Sensor Networks Architecture”, 2009.
13. Filippe C. Jabour, “Mobility support for wireless sensor networks”, 2007