Journal of Advances in Science and Technology

Vol. VII, Issue No. XIV, August-2014, ISSN 2230-9659

"SECURITY IN WIRELESS SENSOR NETWORKS SYSTEM"

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

Journal of Advances in Science and Technology
Vol. VII, Issue No. XIV, August-2014, ISSN 2230-9659

"Security in Wireless Sensor Networks System"

Pradeep Kumar

Assistant Professor, Sityog Institute of Technology, Aurangabad, Bihar

Abstract – In this paper we present about security in wireless sensor networks system. The wireless sensor networks are a novel type of networked systems exemplifies by severely embarrassed computational and energy resources, and an ad hoc operational surroundings. Wireless sensor networks require for effectual security methods. Security in sensor networks pretense different challenges than traditional network/ computer security. There is currently enormous research potential in the field of wireless sensor network security.

Keywords: Wireless sensor network, Security, firewall

----------♦----------

INTRODUCTION

A wireless sensor network is a group of specialized transducers with a communications infrastructure for monitoring and recording conditions at diverse locations. Commonly monitored parameters are temperature, humidity, pressure, wind direction and speed, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentrations, pollutant levels and vital body functions.

A sensor network consists of multiple detection stations called sensor nodes, each of which is small, lightweight and portable. Every sensor node is equipped with a transducer, microcomputer, transceiver and power source. The transducer generates electrical signals based on sensed physical effects and phenomena. The microcomputer processes and stores the sensor output. The transceiver receives commands from a central computer and transmits data to that computer.

A network is connected by many different devices. All providing different services and used to give different types of systems, in different locations or the same location, the ability to communicate. It is important to familiarize yourself with the major devices that allow communication. It also would be good to study the different network topologies and understand how they work.

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions. A WSN system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes. The wireless protocol you select depends on your application requirements. Some of the available standards include 2.4 GHz radios based on either IEEE 802.15.4 or IEEE 802.11 (Wi-Fi) standards or proprietary radios, which are usually 900 MHz.

SECURITY CHALLENGES FOR WIRELESS SENSOR NETWORKS

Wireless sensor networks processing sensitive data are facing the risks of data manipulation, data fraud and sensor destruction or replacement. This concerns applications such as the gathering of data on environmental pollution around industrial installations, or sensor systems replacing traditional video monitoring. Large-scale deployment in practice is conditioned by solving these kinds of security problem and reducing the risks due to limited physical protection of the devices and openness of the wireless communication channel. While modern cryptography and computer security offer many ways of solving these problems, they are focused on solutions for high-performance devices, and not for computationally weak sensors with limited communication bandwidth. New 'lightweight' solutions tailored for the special needs of wireless sensor networks have to be designed. This is one of the focal points of the EU project FRONTS (Foundations of Adaptive Networked Societies of Tiny Artefacts). Fortunately, some recent developments have shown that without heavy cryptographic technology it is still possible to achieve a fair level of security in a practical sense. This report indicates a few ideas of this kind.

Due to the energy required for transmission over long distances, it is often a good idea to route data along a sensor network by making many hops over small distances instead of a direct transmission from a sensor to the sink node. However, such a solution

has the disadvantage that an adversary can attack the network by gaining control over intermediate sensor nodes. The cryptography used by such devices is usually weak and can provide opportunities to reveal information sent or to manipulate them.

The following idea may be applied in order to make it much more difficult to carry out attacks. Instead of a single information path, each message is sent over a double path. This means that instead of a single ith node N_i we have two nodes: P_i and R_i. The encryption scheme has the following basic properties when processing a message M:

- P_{i+1} receives encrypted messages from P_i and R_i in order to compute its share of message M,
- R_{i+1} receive different encrypted messages from Pi and Ri in order to compute its share of M.

The encryption scheme guarantees that corrupting either P_i or R_i reveals no information about M. Also, combining the shares from different stages of message processing gives no information about M as long as the adversary has only one share from each level of the path.

APPLICATIONS

Engineers have created WSN applications for areas including health care, utilities, and remote monitoring. In health care, wireless devices make less invasive patient monitoring and health care possible. For utilities such as the electricity grid, streetlights, and water municipals, wireless sensors offer a lower-cost method for collecting system health data to reduce energy usage and better manage resources. Remote monitoring covers a wide range of applications where wireless systems can complement wired systems by reducing wiring costs and allowing new types of measurement applications. Remote monitoring applications include:

- Environmental monitoring of air, water, and soil
- Structural monitoring for buildings and bridges
- Industrial machine monitoring
- Process monitoring
- Asset tracking

WSN Security

Simplicity in Wireless Sensor Network with resource constrained nodes makes them extremely vulnerable to variety of attacks. Attackers can eavesdrop on our radio transmissions, inject bits in the channel, replay previously heard packets and many more. Securing the Wireless Sensor

Network needs to make the network support all security properties: confidentiality, integrity, authenticity and availability. Attackers may deploy a few malicious nodes with similar hardware capabilities as the legitimate nodes that might collude to attack the system cooperatively. The attacker may come upon these malicious nodes by purchasing them separately, or by "turning" a few legitimate nodes by capturing them and physically overwriting their memory. Also, in some cases colluding nodes might have high-quality communications links available for coordinating their attack. Sensor nodes may not be tamper resistant and if an adversary compromises a node, she can extract all key material, data, and code stored on that node. While tamper resistance might be a viable defense for physical node compromise for some networks, we do not see it as a general purpose solution. Extremely effective tamper resistance tends to add significant per-unit cost, and sensor nodes are intended to be very inexpensive [1] [2] [3] [4].

A Wireless Sensor Network (WSN) can be defined as a group of independent nodes, communicating wirelessly over limited frequency and bandwidth [5]. The novelty of WSNs in comparison to traditional sensor networks is that they depend on dense deployment and coordination to execute their tasks successfully. This method of distributed sensing allows for closer placement to the phenomena to be achieved, when the exact location of a particular event is unknown, than is possible using a single sensor [6]. Consider the Crossbow "MICAz" mote [7], currently a typical mote used in WSNs. It consists of a battery, microprocessor (Atmega128), RF transceiver, ADC, 128K bytes Program Flash Memory and 4K bytes EEPROM. It is evident that there are limitations to what can be achieved through networking a number of these motes. Areas such as power management, network discovery, control and routing, collaborative signal and information processing, tasking and querying, and security are all currently under research [8].

Battery powered nodes are a common feature of many WSN applications, where recharging or replacement would not normally be feasible, and so are considered to be disposable. Many methods of powering these devices have been explored, including solar power, but they remain to be seen typically as "one-use" devices [9].

Eventual failure is expected and so maximizing their lifetime and productivity is extremely important. This notion of battery conservation extends to the primitives used to enforce security in WSNs. Security protocols strive to be light-weight, in terms of code size and processing requirements, whilst retaining their usefulness, in order to assist in achieving this goal.

NETWORK SECURITY TOOLS

There are many different tools that can be used to help secure a network as well as monitor it for malicious activity. There is no "one size fits all" solution that can be applied to all networks. As such it is important to be familiar with the different types of tools that are available. The decision about which is best to use should be based on what our protecting and what we can afford. This should then be compared to what the total cost of ownership will be. Here are some of the different tools we should become familiar with:

Network Based Firewalls

- Stateful Inspection
- Packet filter
- Proxy

Host Based Firewalls

- Software Based
- Hardware Based

Network Based IDS's

- Anomaly Based
- Signature Based

Host Based IDS's

- Application Specific
- Monitoring of Logs, processes and files

CONCLUSION:

In this paper we found that the security in Wireless Sensor Network is very important to the receiving and makes use of sensor networks. In exacting, Wireless Sensor Network manufactured merchandise in industry will not get getting unless there is a fool proof security to the network. WSNs form a particular class of ad hoc networks that operate with little or no infrastructure.

REFERENCES:

[1] S. Sharma, “Energy-efficient Secure Routing in Wireless Sensor Networks”, Dept of Computer Science and Engineering, National Institute of Technology Rourkela, Rourkela, Orissa, 769 008, India, 2009.

[2] D. Boyle, T. Newe,”Securing Wireless Sensor Networks: Security Architectures”, Journal of Networks, 2008, 3 (1). International Journal of Next-Generation Networks (IJNGN),Vol.1, No.1, December 2009 10

[3] X. Du, H. Chen, "Security in Wireless Sensor Networks", IEEE Wireless Communications, 2008.

[4] J. Granjal, R. Silva, J. Silva, "Security in Wireless Sensor Networks", CISUC UC, 2008.

[5] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., Cayirci, E. (2002) ‘A Survey on Sensor Networks’, IEEE Communications Magazine, 40(8), 102-114.

[6] Bharathidasan, A., Anand, V., Ponduru, S. (2001), Sensor Networks: An Overview, Department of Computer Science, University of California, Davis 2001. Technical Report.

[7] Crossbow Technologies Inc. (2007) MICAz [online], available: http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/6020-0060-01_A_MICAz.pdf [accessed 7 Dec 2007].

[8] Chee-Yee Chong, and Kumar, S. P. (2003), “Sensor Networks: Evolution, Opportunities, and Challenges”, Proceedings of the IEEE, Vol. 91, No. 8, August 2003: IEEE, 1247-1256.

[9] https://isc.sans.edu/presentations/first_things_first.html

[10] http://www.ni.com/white-paper/7142/en/