Operation and Restriction on Wireless Sensor Network

[1]Sanjay Kumar, [2]Dhiraj Kumar Banwal

[1]Dept. of CE, Govt. Polytechnic, Narendra Nagar (TG), UK, India

[2]Dept. of IT, Govt. Polytechnic, Narendra Nagar (TG), UK, India

Abstract

In Wireless Sensor Network or WSN the basic issues associated with it is sensors network topology and hardware architecture and it is still open for research. The intent of this paper is to investigate the limitations that affect the efficient operation of WSN, particularly when implementing security techniques, and more challenges that need to be taken into consideration to build efficient WSN.

Keywords

WSN, Security, Limitations, AD-Hoc Sensor Network, Encryption, Storage Restriction, Topology, Hostile Environment

I. Introduction

Wireless Sensor Networks have recently emerged as a hot, new research area in the broad field of (wireless) computer networking. Research interest in WSN has been stimulated by the very recent advances in the Micro-Electro-Mechanical Systems (MEMS) and the wireless communications technology, which have made it possible to produce low-cost, tiny-sized sensors with wireless networking capabilities. WSN are expected to be ubiquitous in the future, with wide deployment both in the military and the commercial sectors.

Researchers envisage a large set of futuristic applications to be made possible with the aid of WSN. In particular, they promise that WSN will revolutionize the way humans interact with their physical surroundings. Some examples of such applications include military applications e.g. battlefield surveillance, friendly or hostile forces tracking, monitoring of equipment, environmental monitoring e.g. flood or forest fire detection, space exploration, biological attack detection, health applications e.g. integrated patient monitoring, diagnostics, tracking and monitoring doctors and patients inside a hospital and many other commercial applications e.g. home / office smart environments, environmental control in buildings.

Wireless AD-Hoc Sensor Networks are a vastly unexplored area. The current focus of research is predominantly directed towards the Power aware or energy efficient routing for WSN, Development of distributed middleware architectures for WSN and Distributed aggregation applications. Design of cross-layer algorithms for improved power efficiency

II. Limitations

The sensor networks are often used in mission critical environments such as in military and healthcare applications. As we can understand, these environments have demanding security requirements that must be addressed at the initial phase of design, in an attempt to focus on a spherical security strategy that will cover as many security problems as possible.

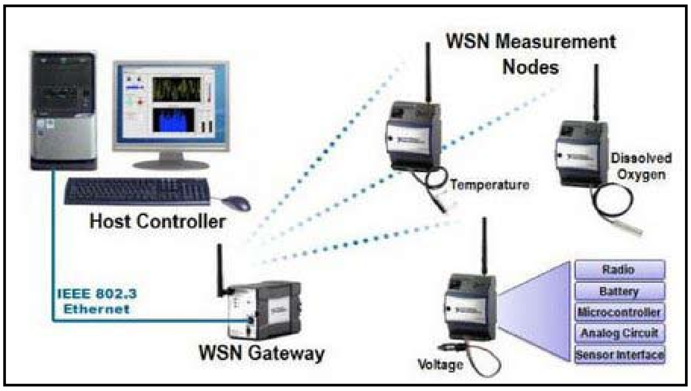

Fig. 1: Communication Network Between Host Controller and Sensor Network

A number of security issues exist in WSN and need to be analyzed in detail in order to design appropriate security mechanisms and overcome security problems that arise in the sensor environment. However, designing new security protocols and mechanisms is constrained by the capabilities of the sensor nodes. This section discusses the limitations that complicate the security design and deployment in sensor networks. It is important to understand the constrained capabilities of sensor nodes if you wish to develop proper security that balances demanding security performance against sensor nodes limitations.

III. Power Restrictions

The power restrictions of sensor nodes are raised due to their small physical size and lack of wires. Since the absence of wires results in lack of a constant power supply, not many power options exist. Sensor nodes are typically battery-driven. However, because a sensor network contains hundreds to thousands of nodes, and because often WSN are deployed in remote or hostile environments, it is difficult to replace or recharge batteries. The power is used for various operations in each node, such as running the sensors, processing the information gathered and data communication.

Keep in mind that communication between sensor nodes consumes most of the available power, much more than sensing and computation. Power limitations greatly affect security, since encryption algorithms introduce a communication overhead between the nodes; more messages must be exchanged, i.e. for key management purposes, but also messages become larger as authentication, initialization and encryption data must be included.

IV. Limited Computational Power

In the case of computational power, computations are linked with the available amount of power. Since there is a limited amount of power, computations are constrained also. Although it is acknowledged that sensors are not expected to have the computing power of workstations or even mobile handheld devices, researchers and developers are greatly concerned with the issue.

The more power is used for communication than computations. Therefore, since the power for computations is even more constrained than the total quantity of power, complex security solutions are prohibited? The limitation of computational power limits the adoption of strong cryptographic algorithms such as the RSA public key algorithm, which is computationally expensive. Instead, symmetric encryption algorithms are used to secure sensor nodes' communication, since symmetric encryption doesn't have as demanding computational requirements as asymmetric encryption. However, with asymmetric encryption, features like digital signatures are not supported. Therefore, another challenge for researchers and developers is to design appropriate algorithms to establish and verify trust among the nodes participating in a communication. Furthermore, other security solutions must be adopted to cover the weaknesses of symmetric encryption; when an adversary compromises a node, he could retrieve the shared key used to encrypt the messages and then compromise the entire communication of the sensor network.

V. Storage Restrictions

The limited capability for storage affects the storage of cryptographic keys as well. According to the encryption scheme used, each sensor node may need to know a number of keys for each other node in the network to secure communication, and thus store the keys in the nodes' storage space. However, the large number of sensor nodes requires a lot of memory, which may not be provided. As I mentioned previously, having a single encryption key common to all nodes allows an adversary to compromise the whole network by compromising only a single node. The challenge of storage restriction is for researchers to design security protocols in a way that a minimum number of encryption keys must be used to provide adequate protection to the network.

VI. Design Challenges in Wireless Sensor Network

The design challenges include the scalable and flexible architecture, error prone wireless medium and Fault tolerance and adaptability.

A. Scalable and Flexible Architecture

The network should be scalable and flexible to the enlargement of the network's size. The communication protocols must be designed in such a way that deploying more nodes in the network does not affect routing and clustering. Rather, the protocols must be adapted to the new topology and behave as expected. In other words, the network must preserve its stability. Furthermore, introducing more nodes into the network means that additional communication messages will be exchanged, so that these nodes are integrated into the existing network. This must be done in a way that a minimum number of messages need to be exchanged among the sensor nodes, and thus battery is not wasted unreasonably.

B. Error-prone Wireless Medium

Since sensor networks can be deployed in different situations, the requirements of each different application may vary significantly. Researchers must take into consideration that the wireless medium can be greatly affected by noisy environments, and thus the signal attenuates in regard to the noise. Note that an adversary can intentionally interfere and cause enough noise to affect the communication. In an environment such as healthcare, it is vital to ensure that communication is on time to respond to emergencies.

C. Fault Tolerance and Adaptability

If a sensor node fails due to a technical problem or consumption of its battery, the rest of the network must continue its operation without a problem. Researchers must design adaptable protocols so that new links are established in case of node failure or link congestion. Furthermore, appropriate mechanisms should be designed to update topology information immediately after the environment changes so as to minimize unnecessary power consumption.

VII. Hostile Environment

Sensor networks can be deployed in remote or hostile environments such as battlefields. In these cases, the nodes cannot be protected from physical attacks, since anyone could have access to the location where they are deployed. An adversary could capture a sensor node or even introduce his own malicious nodes inside the network. If the latter is the case, the adversary's aim is to trick the network into accepting his nodes as legitimates.

In either case, the adversary can compromise sensitive information, which is either stored on the compromised nodes or is forwarded through the adversary's nodes to the next hop; the sensitive information that is collected could be used for illegal purposes. The challenge here for researchers and developers is to design resilient security protocols and solutions offering security, even if a subset of sensor nodes are compromised. It is important to ensure that, if a node is compromised, sensitive information stored on the node cannot be taken off with ease.

VIII. Random Topology

Most of the time, deploying a sensor network in a hostile environment is done by random distribution, i.e. from an airplane. Therefore, it is difficult to know the topology of sensor networks a priori. In these situations, it is hard to store various encryption keys on nodes in order to establish encryption among a group of neighbors, since the neighborhood cannot be known a priori.

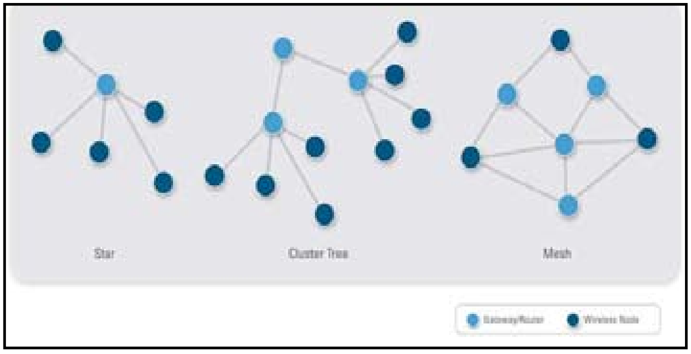

Fig. 2: Gateway and Wireless Node Topology

The challenge is to design key agreement protocols that do not require certain nodes to be neighbors of some other nodes, and also do not require encryption keys to be stored on sensors before deployment. Appropriate key distribution algorithms must be designed along a flexible WSN architecture to securely provide encryption keys in real time.

IX. Conclusion

In this paper we discussed some challenging directions that need special attention. Focus should be placed on designing protocols that are scalable, flexible, fault tolerant and adaptable to dynamic changes. However, the main challenge for researchers is to balance the trade off between resources spent for security and the protection offered. The target is to have a spherical security strategy with solutions that compensate each others' vulnerabilities, and provide an enhanced protection to the network and its information.

References

[1] Akyildiz, I., Su, W., Sankarasubramaniam, Y., Cayirci, E.,"A Survey on Sensor Networks", IEEE Communications Magazine, August 2002.

[2] Balenson, D., et al,"Communications Security Architecture for Army Sensor Networks", NAI Labs T.R. #00-016, September 30, 2000.

[3] Carman, D., Kruus, P., Matt, B.,"Constraints and Approaches for Distributed Sensor Network Security", NAI Labs T.R. #00-010, June 1, 2000.

[4] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. Tygar. "SPINS: Security Protocols for Sensor Networks", In Seventh Annual ACM International Conference on Mobile Computing and Networks (Mobicom 2001), Rome Italy, July 2001.

[5] S. Basagni, K. Herrin, D. Bruschi, E. Rosti,"Secure pebblenets", In Proceedings of the 2001 ACM International Symposium on Mobile Ad-Hoc Networking and Computing, pp. 156-163. ACM Press, October 2001.

[6] Jeffery Undercoffer, Sasikanth Avancha, Anupam Joshi and John Pinkston,"Security for Sensor Networks", 2002 CADIP Research Symposium, [Online] Available: http://www.csee.umbc.edu/cadip/2002Symposium/.

[7] N. Asokan, P. Ginzboorg,"Key Agreement in Ad Hoc Networks", Computer Communications, Volume 23, pp. 1627-1637.

[8] L. Zhou, Z. J. Haas,"Securing Ad-Hoc Networks", IEEE Networks, Vol. 13, Issue 6, 1999.

[9] J. Kong, P. Zerfos, H. Luo, S. Lu, L. Zhang,"Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks", IEEE ICNP 2001.

[10] C. Perkins,"Ad-Hoc Networks", Addison-Wesley, Reading, MA, 2000.

[11] A. D. Wood, J. A. Stankovic,"Denial of Service in Sensor Networks", IEEE Computer, October 2002, pp. 54-62.

[12] C. Gehrmann,"BluetoothTM Security White Paper", White paper, Bluetooth SIG Security Expert Group, Apr 2002.

[13] Y. W. Law, S. Dulman, S. Etalle, P. Havinga,"Assessing Security-Critical Energy-Efficient Sensor Networks", Department of Computer Science, University of Twente, Technical Report TR-CTIT- 02-18, Jul 2002.

[14] Y.-C. Hu, A. Perrig, D. B. Johnson. Ariadne,"A Secure On-Demand Routing Protocol for Ad Hoc Networks", Technical Report TR01-383, Department of Computer Science, Rice University, 2001.

[15] Zheng Yan, (Networking Laboratory, Helsinki University of Technology),"Security in Ad Hoc Networks", [Online] Available http://citeseer.nj.nec.com/536945.html.

[16] Pietro Michiardi, Refik Molva,"Prevention of Denial of Service attacks and Selfishness in Mobile Ad Hoc Networks", Research Report No RR-02-063, January 2002.

[17] T. Aura, P. Nikander, J. Leiwo,"DOS-Resistant Authentication with Client Puzzles", Proc. Security Protocols Workshop 2000, Springer-Verlag, New York, 2000, pp. 170-177.

[18] S. Marti, T. Giuli, K. Lai, M. Baker,"Mitigating routing misbehavior in mobile ad hoc networks", In Proceedings of MOBICOM, 2000.

[19] P. Michiardi, R. Molva,"Core: A Collaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks", In Communications and Multimedia Security Conference, 2002.

[20] P. Michiardi, R. Molva,"Prevention of denial of service attacks and selfishness in mobile ad hoc networks", Research Report RR-02-063, Institut Eur´ecom, France, 2002.

[21] P. Michiardi, R. Molva,"Simulation-based analysis of security exposures in mobile ad hoc networks", In European Wireless 2002: Next Generation Wireless Networks: Technologies, Protocols, Services and Applications, February 25-28, 2002, Florence, Italy, 2002.

[22] L. Blazevic, L. Buttyan, S. Capkun, S. Giordano, J.- P. Hubaux, J.-Y. Le Boudec,"Self-organization in mobile ad hoc networks: the approach of terminodes", IEEE Communications Magazine, 39(6), pp. 164–174, June 2001.

[23] L. Butty´an, J.-P. Hubaux. Nuglets,"A Virtual Currency to Stimulate Cooperation in Self- Organized Mobile Ad Hoc Networks", Technical Report DSC/2001/001, Department of Communication Systems, Swiss Federal Institute of Technology, 2001.

[24] S. Buchegger, J.-Y. Le Boudec,"Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks", In Proceedings of the 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing, Canary Islands, Spain, January 2002.

Mr. Sanjay Kumar Is working as HOD in Department of CSE in Govt. Polytechnic, Narendra Nagar (TG) Under the Department of Technical Education, Govt. of Uttarakhand. (India), He have Eleven year Experience of teaching in Govt. as well as Private Engg. College and he also worked as examination controller in Uttarakhand Board of Technical Education, Roorkee.

Mr. Dhiraj Kumar Banwal is working as Lecturer in Department of IT in Govt. Polytechnic, Narendra Nagar (TG) Under the Department of Technical Education, Govt. of Uttarakhand, India. He have Nine year Experience of teaching in Govt. as well as Private Engg. College and he also worked as examination controller in Engg. College And he had external practical examiner of IGNOU.