Some Security Aspects at Wireless Sensor Networks

Irfan Shaqiri

Abstract - In this paper we discuss some security threats, attacks, countermeasures and challenges faced by Wireless Sensor Networks. They have become a wide field of research and development because of the enormous number of applications that can highly profit from such systems and has led to the development of cheap, available and self-contained battery powered computers, known as sensor nodes or "motes", which can accept input from an attached sensor, process this input data and transmit the results wirelessly to the transit network. Despite making such sensor networks possible, wireless nature of the sensors presents a number of security threats when deployed for certain applications like healthcare ,surveillances, military etc. The issue of security is as result of the wireless nature of the sensor networks and restricted nature of resources on the wireless sensor nodes, which means that security architectures used for traditional wireless networks are not applicable. Also, wireless sensor networks have an additional vulnerability because nodes are often located in enemy or dangerous environment where they are not physically protected by anyone.

Index Terms: WSN, Applications, Healthcare, Security, Sensor, Nodes, Motes.

1 INTRODUCTION

Sensor networks are highly distributed networks of small, lightweight wireless nodes, deployed in large numbers to monitor the environment or system by the measurement of physical parameters such as temperature, pressure, or relative humidity. Building sensors have been made possible by the recent advances in micro-electromechanical systems (MEMS) technology. The sensor nodes are similar to that of a computer with a processing unit, limited computational power, limited memory, sensors, a communication device and a power source in form of a battery. In a typical application, a WSN is scattered in a region where it is meant to collect data through its sensor nodes [1]. The applications of sensor networks are endless, limited only by the human imagination. In this paper an overview on various WSN attacks are mentioned. Summary on the counterattacks and possible preventive measures are mentioned.

It is to be mentioned that all the attacks has been described thoroughly as well as the preventive measures which should be taken in order to make these networks more secure for use.

2 SECURITY REQUIREMENTS

2.1 Data Authentication

As sensor networks use a shared wireless communication medium, authentication is necessary to enable sensor nodes to detect all malicious injected packets. Authentication enables a node to verify the origin of a packet (source authentication) and ensure data integrity, which is in fact to verify that whole flow of data is unchanged (data authentication) [2]. From one point of view, for healthcare, military and safety-critical applications, the adversary has clear incitement to inject false data reports or malicious routing information; on the other hand, even for civilian applications such as office/home applications where we expect a relatively non adversarial environment, it is still risk prone to go without authentication, for then people only moderately skilled would be able to meddle with the sensor network protocols solely out of mischief.

Notwithstanding authentication prevents outside attackers from injecting or spoofing packets, it does not solve the problem of compromised nodes [3]. As a compromised node has the secret keys of a legitimate node, it can authenticate itself to the network. Nevertheless, we may be able to use intrusion detection techniques to find the compromised nodes and revoke their cryptographic keys network-wide.

2.2 Data Secrecy

Securing the secrecy of sensed data is very important action for protecting data from eavesdroppers and other attacks. We can use standard encryption functions (e.g., the AES block cipher) and a shared secret key between the communicating parties to achieve secrecy. However, encryption itself is not sufficient for protecting the privacy of data, as an eavesdropper can perform traffic analysis on the overheard ciphertext, and this can release sensitive information about the data. In addition to encryption, privacy of sensed data also needs to be enforced through access control policies at the base station to prevent misuse of information [4]. Consider, for example, a person who has glucose sensor for measuring level of glucose in his blood at so called in-body applications. Sensor is implanted in his body to sense the level of glucose, and the information is sent to a Web server to answer requests for level of glucose in his blood. Generally, people would like to limit the right to access their health condition to small group of people as are physicians. Therefore, access control has to be enforced at the Web server to prevent misuse of information by unintended parties.

2.3 Data Availability

Providing availability requires that the sensor network be

functional throughout its lifetime. Denial-of-service (DoS) attacks often result in a loss of availability. In practice, loss of availability may have serious impacts. In a manufacturing monitoring application, loss of availability may cause failure to detect a potential accident and result in financial loss; in a healthcare applications may cause failure to detect level of glucose in blood or temperature result where we can have serious implications for health of patients, loss of availability may open a back door for enemy invasion. Different attacks can compromise the availability of the sensor network. When considering availability in sensor networks, it is important to achieve agreeable degradation in the presence of node compromise or benign node failures [5].

2.4 Self-Organization

A wireless sensor network is a typically an ad hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security [6]. If self-organization is missing in a sensor network, the damage resulting from an attack or even the risky environment may be destructive.

3 Attacks on Wireless Sensor Networks

The threats and attacks against sensor networks in general can be broadly classified into two major categories – passive and active. Regarding passive attacks can occur while routing the data packets. The attackers may change the destination of packets or make routing to be conflicting. In this case, the attackers can also steal the health data by eavesdropping to the wireless communication media [7]. The active threats are more harmful and dangerous then their passive counter parts. Criminal minded people may find the location of the user by eavesdropping. This may lead to life threatening situations. The normal trend of sensor device design is that they have little external security features and hence are prone to physical tampering. This increases the vulnerability of the devices and poses rougher security challenges. Similarly vital data transmission from WBAN networks or other applications through GPRS or similar networks can be stolen by eavesdropping [8].
The following are the types of attacks on wireless sensor networks:

- Common Attacks
- Denial of service (DOS) Attack
- Node compromise
- Impersonation Attack
- Protocol- specific Attack
- Blackhole/Sinkhole Attack

3.1 Common Attack

The first common attack is eavesdropping i.e. an adversary can easily retrieve valuable data from the transmitted packets that are sent. The second common attack is Message modification i.e. the adversary can intercept the packets and modify them. The third common attack is message replay i.e. the adversary can retransmit the contents of the packets at a later time.

3.2 DOS Attack

The ordinary DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. A DOS attack on WSN may take several forms. The first one is node collaboration, in which a set of nodes act maliciously and prevent broadcast messages from reaching certain sections of the sensor networks [11]. The second one is jamming attack, in which an attacker jams the communication channel and avoids any member of the network in the affected area to send or receive any packet. The third one is exhaustion of power, in which an attacker repeatedly requests packets from sensors to deplete their battery life.

3.3 Node compromise Attack

A sensor node is said to be compromised when an attacker gains control or access to the sensor node itself after it has been deployed. A lot of different complex attacks can be easily launched from compromised nodes, since the subverted node is a full- fledged member of the sensor network [12].

3.4 Impersonation Attack

The most common attack that can be launched using a compromised node is the impersonation attack, in which a malicious node impersonates a legitimate node and uses its identity to mount an active attack such as Sybil or node replication. In a Sybil attack, a single node takes on multiple identities to deceive other nodes [14]. On the other hand, the node replication attack is the duplication of sensor nodes.

3.5 Protocol- specific Attack

The attacks against routing protocols in WSN are: Spoofed routing information- corruption of the internal control information such as the routing tables, Selective forwarding- selective forwarding of the packets that traverse a malicious node depending on some criteria, Wormhole attack- Creation of a wormhole that captures the information at one location and replays them in another location either unchanged or tampered, Hello flood attack- creation of false control packets during the deployment of the network [15].

3.6 Blackhole/Sinkhole Attack

In this attack, a malicious node acts as a blackhole to attract all the traffic in the sensor network. Especially in a flooding based protocol, the attacker listens to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. Once the malicious device has been

able to insert itself between the communicating nodes (for example, sink and sensor node), it is able to do anything with the packets passing between them [17]. Actually, this attack can affect even the nodes which are considerably far from the base stations.

4 DEFENDING AGAINST ATTACKS

At any design of healthcare, military or other applications for sensor networks, security issues must be resolved firstly otherwise they may give rise to serious problems as discussed earlier. To counter the major threats two broad level security measures can be applied–encryption and authentication mechanisms. Any communication of personal health or other information's and data over the networks must be encrypted [18]. Furthermore as mentioned by many authors , preventing unauthorized modifications of data while at the same time ensuring that only legitimate devices can create and inject data to the network prevents many of the previously discussed attacks. Authentication mechanisms can be used to ensure the data is coming from the person/entity is claiming to be from right person.

In healthcare application scenario, where a person wears various devices, we can use a centralized control device for data transmission from in and out of the network. This device can also act as the gateway between the internal network and outside world communication [19]. Security measures such as authentication, firewalls and other controls can be applied at the controller level to monitor the traffic. Security in sensor networks applications in healthcare cannot be compromised. Warily constructed measures are necessary in this regard. We feel that security protection measures may be applied in three levels – Administrative, Physical and Technical.

• Administrative level security: at this level, security measures has to be taken for security breaches by the trained staff or people responsible for system operation. A well-defined user hierarchy along with strong authentication measures may prevent security breaches. Therefore these important security measures must include different types of access mechanisms so that only authorized users can access the data. Also, it may be a case where data forwarding may be only to the place or people which are previously authorized.

• Physical level security: at this level, measures may include controlling access to physical devices and data in the system for supposed stealing or tampering. Devices may be vulnerable from both people with malicious minds or from natural causes such as wear and tear [20]. Therefore, careful designing of devices to make them tamper proof is also necessary. But it is also understood that avoiding physical tampering of devices is hard to achieve. Another preventive measure can be that only authorized people should be allowed to physically handle the devices while they are operation. Users must be strongly advised regarding these types of security measures which should be taken.

• Technical level security: technical level, security checks are necessary for wireless communications and propagation of information. If the network is such that data is sent to central servers, server based security measures be used at the server side and client based security at the user side. This may again increase load on sensors at the user side and thereby increase the overall cost. So we also must take care of this aspect. It is also likely that more powerful motes will need to be designed in order to support the increasing requirements for computation and communication. Securing the routing of data can also be applied as a security measure [21]. Wireless networks are very much susceptible to intrusion. Intrusion detection and prevention techniques are therefore required in these networks. Due to the sensitive nature of military, healthcare or other applications, extra measures such as encryption of data, and constant monitoring of the network is necessary. While monitoring may not be a cost effective measure, encryption and creation of secure user groups can be effective as well as cost saving. Routing is another area where technical level security is required. If the data is sent to some remote host (e.g., doctors or some other hospital computers), routing is necessary. Attackers may cause routing inconsistencies resulting in wrong destinations and receiving of wrong data. Hence proper routing protocol and management is necessary to prevent such attacks [25]. At the end, it must be noted that end to end security is compulsory to make the wireless sensor networks in military, healthcare or other applications usable and acceptable by the common people. Threats such as tampering with data, Denial of Service (DoS), physical tampering, eavesdropping and others need far more special attention than any other common networks.

5 CONCLUSIONS

In this paper we have discussed privacy and security issues that arise when integrating these new technology into a lot of systems as in healthcare, automotive industry, military systems, agriculture etc. We have also mentioned security requirements, which should be met during operation of this applications and in same time, type of threats and countermeasures against them. Considering that wireless sensor networks is growing and become so popular and common, we hope that further expectations of security will be required with the only goal, data to be more secured during transfer process from one node to another.

REFERENCES

[1] M. Li, W. Lou and K. Ren, "Data security and privacy in wireless body area networks", Wireless Communications, IEEE, Feb 2010

[2] Mohammad Sayad Haghighi , Kamal Mohamedpour, (2008), Securing Wireless Sensor Networks against Broadcast Attacks, IEEE

[3] Adrian Perrig, John Stankovic, David Wagner, "Security in Wireless Sensor Networks" Communications of the ACM, Page53-57, year 2004

[4] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", International conference on Advanced Computing Technologies,Page1043-1045, year 2006

[5] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", AdHoc Networks (elsevier), Page: 299-302, year 2003

[6] Ian F. Akykildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, "A Survey on Sensor Networks", IEEE Communication Magazine, year 2002

[7] John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, "Wireless Sensor Network Security: A Survey", Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), Page3-5, 10-15, year 2006

[8] Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong, "Security in wireless sensor networks: issues and challenges" Advanced Communication Techno ogy (ICACT), Page(s):6, year 2006

[9] Tahir Naeem, Kok-Keong Loo, Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks, International Journal of Digital Content Technology and its Applications, Page 89-90 Volume 3, Number 1, year 2009

[10] Undercoffer, J., Avancha, S., Joshi, A. and Pinkston, J. "Security for sensor networks". In Proceedings of the CADIP Research Symposium, University of Maryland, Baltimore County, USA, year 2002 http://www.cs.sfu.ca/~angiez/perso nal/paper/sensor-ids.pdf

[11] Zia, T.; Zomaya, A., "Security Issues in Wireless Sensor Networks", Systems and Networks Communications (ICSNC) Page(s):40 – 40, year 2006

[12] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou, Sensor Network Security: A Survey, IEEE Communications Surveys & Tutorials, vol. 11, no.2,page(s): 52-62, year 2009

[13] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.

[14] D. Djenouri, L. Khelladi, and N. Badache, "A Survey of Security Issues in Mobile ad hoc and Sensor Networks," IEEE Commun. Surveys Tutorials, vol. 7, pp. 2–28, year 2005.

[15] S. Schmidt, H. Krahn, S. Fischer, and D. Watjen, "A Security Architecture for Mobile Wireless Sensor Networks," in Proc. 1st European Workshop Security Ad-Hoc Sensor Networks (ESAS), 2004.

[16] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Commun. Surveys Tutorials, vol. 8, pp. 2–23, year 2006.

[17] Yun Zhou, Yuguang Fang, Yanchao Zhang, Securing Wireless Sensor Networks: A Survey, IEEE Communications Surveys & Tutorials, year 2008

[18] Xiuli Ren, Security Methods for Wireless Sensor Networks, Proceedings of the 2006 IEEE International Conference on Mechatronics and Automation , Page: 1925 ,year 2006

[19] R. Roman, J. Zhou, and J. Lopez, "On the security of wireless sensor networks," in International Conference on Computational Science and Its Applications – ICCSA 2005, May 9-12 2005, vol. 3482 of Lecture Notes in Computer Science, (Singapore), pp. 681–690, Springer Verlag, Heidelberg, D-69121, Germany, 2005.

[20] N. Sastry and D. Wagner, "Security considerations for ieee 802.15.4 networks," in Proceedings of the 2004 ACM workshop on Wireless security, pp. 32–42, Philadelphia, PA, USA: ACM Press, 2004.

[21] 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

[22] Mona Sharifnejad, Mohsen Shari, Mansoureh Ghiasabadi and Sareh Beheshti, A Survey on Wireless Sensor Networks Security, SETIT 2007.

[23] Newsome, J., Shi, E., Song, D, and Perrig, A, "The sybil attack in sensor networks: analysis & defenses", Proc. of the third international symposium on Information processing in sensor networks, ACM, 2004, pp. 259 – 268

[24] Pathan, A-S. K., Alam, M., Monowar, M., and Rabbi, F., "An Efficient Routing Protocol for Mobile Ad Hoc Networks with Neighbor Awareness and Multcasting", Proc. IEEE E-Tech, Karachi, 31 July, 2004, pp. 97-100.

[25] M. Patel and J. Wang, Applications, challenges, and prospective in emerging body area networking technologies, Wireless Communications, IEEE, Feb 2010.

[26] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "SAGE: A strong privacy-preserving scheme against global eavesdropping for ehealth systems," IEEE J. Sel. Areas Commun., vol. 27, no. 4, pp. 365–378, 2009

[27] O. G. Morchon and H. Baldus, "Efficient Distributed Security for Wireless Medical Sensor Networks", International conference on Intelligent Sensors, Sensor Networks and Information Processing, ISSNIP 2008.

[28] D. Singelé e, B. Latré, B. Braem, M. De Soete, P. De Cleyn, and B. Preneel. et al. (2008). A secure cross-layer protocol for multi hop wireless body area networks. 7th International conference on ad-hoc networks & wireless (ADHOCNOW 2008), Vol. LNCS 5198, France, Sep 11–13, 2008, pp. 94–107