www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 5 May 2016, Page No. 16487-16491

Wireless Sensing System Security Concerns - A Review

Shabnum Mohi Ud Din[1], Narender Singh Rana[2]

[1]M. Tech Scholar, Department of Computer Science and Engineering, GITM, Bilaspur, Haryana,

[2]Assistant Professor, Department of Computer Science and Engineering, GITM, Bilaspur, Haryana

[1]Shabnumbhat.bhat@gmail.com

[2]Er.narender.singh@gmail.com

Abstract

Sensors are electronic devices that are meant for recording particular environment variable for example temperature, pressure, speed etc. with the advancement in the field of electronics and sensors, it is possible to the gather physically measured data from sensors remotely. This is possible only because of the network facilities like Ethernet, Wi-Fi, and cellular networks that enable remote access to the data sampled by a sensor.Faults, errors, failures and attacks are common in a wireless communication and this imperfection in wireless communication compromises the effective data collection of a wireless sensing system. In this paper we are going to discuss some various challenges and solutions in robust data collection in wireless sensing system.

Keywords: Wireless sensing, Sensors, Faulty Data, Network attacks, Privacy breach.

I. Introduction:

Sensors being electronic devices capable of sensing and recording particular environment variable like temperature, distance, pressure, speed etc. and the data collected is then transformed into knowledge by software. There are some situations where it is not possible for a human to collect the data for example radioactive environment, war bases, the environments where humans cannot survive but the data sensing and monitoring is very useful to study the various aspects of the environment. So the network advancements are used in such environments to serve the purpose. With the help of such technologies, we are able to collect and transform that data remotely. [1] Using computer networks the data from the sensors can be sent to a nearby station through wireless medium and even further delivered to a remote monitoring center in order to serve purpose of data collection. This can exemplified by a scenario where a patient is under observation for various health parameters let us take monitoring of heart beat, a Bluetooth enabled heart beat sensor can record the heart beat and can send the recorded data to the smartphone, which could be further delivered that data to any remote base using Wi-Fi or cellular network. Wireless medium is prone to various kinds of faults, failures, attacks and errors and hence can compromise the collected data.

DOI: 10.18535/ijecs/v5i5.26

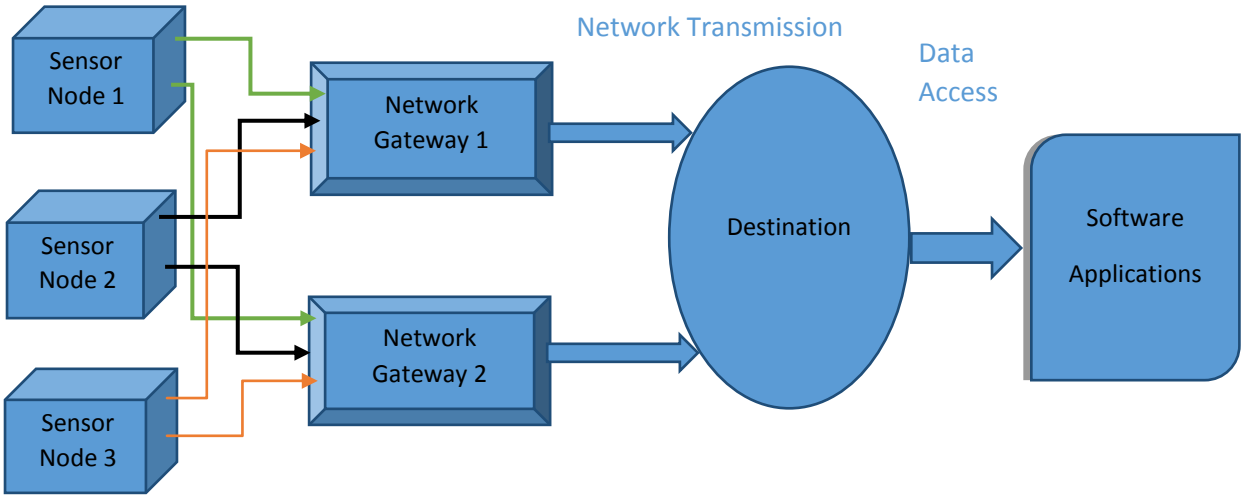

Figure 1: Data Flow in wireless sensor Networks

Figure 1 clearly shows how the data collected, which is collected by the mechanism of sensing, is propagated from sensors through wireless medium to the network gateways. The network gateways further propagate the data to some destinations, typically one. These destinations are generally servers. The software applications can easily access the data from the destinations.In a wireless sensing system, a sensor may be placed indoors, outdoors, or even attached to another device. The sensor may integrate radio capability into its circuit or connect to another device that is wireless-enabled. The gateway devices are not restricted to conventional routers; instead, they can be a smartphone integrating or connected to the sensor, or a networked computer. The gateway devices are free to choose their networks to deliver the data to the final destinations, possibly through computer networks or cellular networks. For applications, the data collected onto the destinations can be accessed by certain software.

II. Data Collection and Corresponding Challenges

As wireless medium is known to be prone to various faults, failures, errors and attacks, so the data collection and propagation can be compromised by such nature of medium of propagation. In order consummate effective data collection and propagation, some of the important issues need to be addressed. In figure 2, illustrates clearly the spots in which these issues make their entry in the wireless sensing system. At the data collection level the sensors may fail to collect the correct data during data sampling. The data from the sensors may get unavailable or may be erroneous. There are two reasons for such erroneous data, which is hardware or software at sensor level. Due to the faults and failures in sensor hardware or software, the erroneous data can be generated and propagated in the wireless system. The second spot where the issue may arise is during data transmission,faults, failures, and attacks might occur. At last the issues may arise at the level of data access, where software applications can access the collected data from destination, there it can be a privacy breach. As the collected data may contain certain private data that can under surveillance of some other interested parties (intruders). In preceding section, all issues will be described in detail with appropriate solutions.

DOI: 10.18535/ijecs/v5i5.26

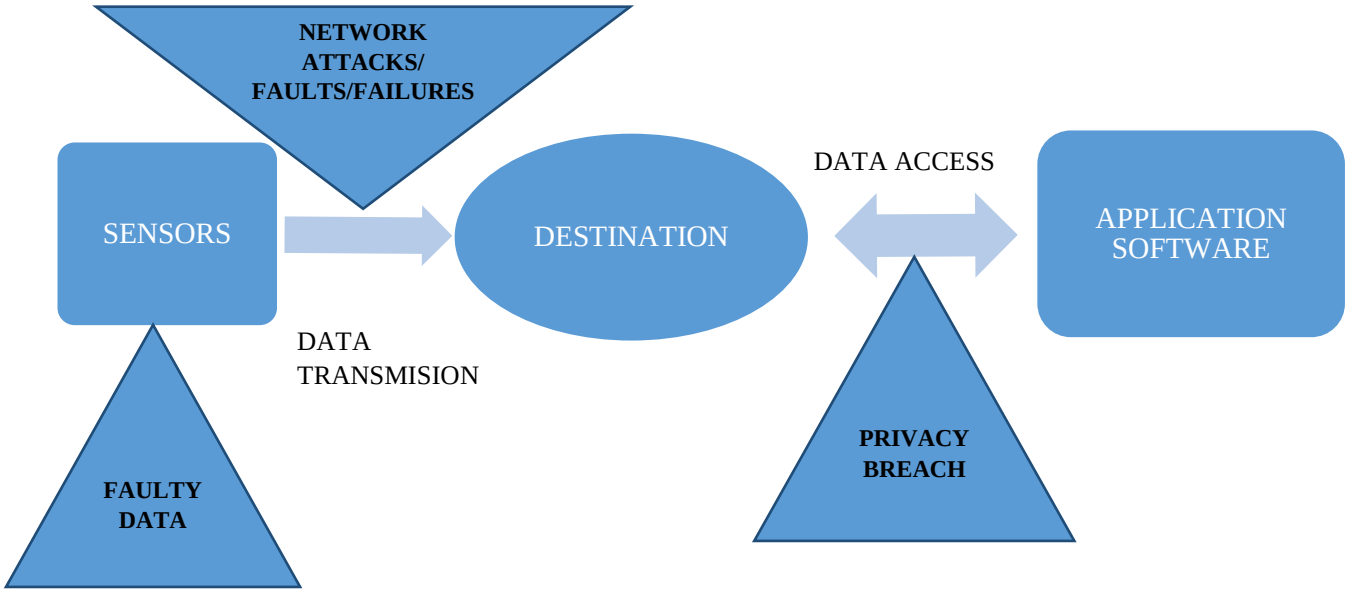

Figure 2 Potential Spots where issues can arise

DATA FAULTS ON THE SENSORS

Sensors are electronic devices manufactured as commodity products by hardware manufactures. Electronic devices are designed and programmed such that it meets certain accuracy requirementon the measured attributes and certain fault tolerance requirement. So the hardware manufacturers are responsible for making the device highly accurate in terms of its functionality. In reality, it is not rear for devices to generate the wrong data. And a malicious sensor will intentionally generate and propagate wrong and erroneous data in the network. In order to prevent such a data to flow through network, we need to have some detection mechanism, to detect errors in the data generated or received through sensors. It is generally been a trend to employtrust management for sensing devices to detect malfunctioning of sensors.[2] Trust management system assigns a trust value sensor toreflect its trustworthiness according to its past performance. The trust management is provedto be effective in improving security concerns of the devices.[3]However, to detect erroneous dataproduced by a sensor, there are a few important issues with directly applying the existingresearch outcomes. First, most trust research focuses on link-level one-hop communicationbehaviors, and data integrity is overlooked. Since data collection is the main task of wirelesssensing systems, the importance of data integrity should never be overlooked. Second,overcomplicated models often render reputation system hard to apply to deployed wireless sensing systems. Those models may cause too much overhead. Finally, the fair treatment ofnew transactions and past behaviors, as adopted in the existing work, suffers various attacks. These issues can be addressed by developing SensorTrust. SensorTrust integrates past history and recent risk to accurately identifythe current trust level. This employs Gaussian mixture model to rank data integrity of the collected data.

NETWORK ISSUES DURING THE DATA TRANSMISSION

The major reason that prevents data from being delivered to the destinations are faults, failures and errors in network transmission. As discussed earlier, there are three spots where the data can be affected by external agencies like environment, hardware impairments, network failures and privacy breach. Out of these faults in data collection, the major risk occurs during network transmission from a sensor to network gateway. As stated earlier, wireless networks are prone to majority of failures and attacks by intruders and imposters, such behavior is normally addressed by the robust routing protocols. The particular characteristics of

Wireless sensing system exasperate these problems.In many applications, especially in a wild environment, the sensors used are battery poweredembedded sensors with limited processing capabilities, such as TelosB motes[4]. With a limited radio communication range, many sensors together with their equipped radiotransceivers, comprise a multi-hop wireless ad-hoc network. To send the data to a networkgateway, each sensor usually wirelessly sends data out to one of its neighboring sensors,which in turn forwards the data to another sensor. The data reach the network gateway viaa multi-hop path through multiple sensors. Such wireless networks consisting of sensors aredefined as wireless sensor networks (WSNs)[5] and we call network gateways as base stations also.Compared to conventional wireless networks, WSNs consisting ofresource-constrained sensors more easily suffer failures and malicious attacks. Most existingnetwork protocols for these networks either assume the honesty of the nodes or focus on howto increase the throughput of the network under faults and failures[6]or attempt to excludeunauthorized participation by encrypting data and authenticating packets[7]. Some of the protocols perform well under the conditions like attacks and faults in networks, but these protocols can be defeated by a malicious attackers by replaying the routing information. A malicious node can participate in process of data generation and collection by using identity of a valid node by replaying their routing information. The multi-hop routing offers very weak protection against the identity deception through replaying of routing information.

PRIVACY PROTECTION ON THE GATHERED DATA

There can be certain scenarios where the information that flows through the sensor networks may be private that cannot be risked to get exposed.An example of these applicationsis the self-monitoring and self-management of patient health[8].In such a wirelesssensing system, users utilize off-the-shelf wireless biomedical sensors to detect their biophysicaldata such as heart rate and the data are sent out to a remote station through theirsmartphones[9]. The remote stations may deliver feedback accordingly back to the users.While such applications can lower the medical cost and facilitate remote diagnoses[10], theyencounter the obstacle of privacy concern[11]. The prevailing wireless sensingsystems in such areas either does not consider privacy protection at all or restrict thecollected data to its internal use only so as to reduce privacy risks. The restriction ofthe internal use of data prevents third-party applications from exploring the data and becomesan obstacle to data sharing. The existing privacy research mainly concerns itself about themechanisms to identify and prevent privacy issues and often does not support arbitrarythird-party applications.

III. CONCLUSION

In this paper, we tried to define various scenarios prevailing in wireless sensing networks, specially related to the security concerns in data collection and transmission in wireless sensing network. In this paper, we tried to specify the spots or regions that are vulnerable to the external effects whether it be the hardware constraints, software constraints related to the sensor nodes or it may be the faults prevailing in the wireless medium for propagation of data from the sensor nodes to the base station or network gateway or it may be the issues related to the data access i.e. who can access what type of data in the network or gathering center. One can apply certain measures to control the security issues in the wireless sensing networks by modifying the present system or designing altogether new system considering the discussed issues in wireless sensing system.

IV. REFERENCES

[1] G. ZHAN, "System support for robust data collection," 2012.

[2] J. F. a. J. L. M. Blaze, "Decentralized trust management.," in *In Proceedings of 1996 IEEE Symposium on Security and Privacy.*, 1996.

[3] K. E.-K. L. X. a. L. K. A. Boukerche, "A novel solution for achieving anonymity in wireless ad hoc networks.," in *In Proceedings of the 1st ACM international workshop on Performance evaluation of*

wireless ad hoc, sensor, and ubiquitous networks, 2004.

[4] C. t. inc..

[5] Y. Y. a. T. Y. V. Rajaravivarma, "An overview of wireless sensor network and applications," in *In System Theory, 2003. Proceedings of the 35th Southeastern Symposium*, 2003.

[6] J. A.-K. a. A. Kamal, "Routing techniques in wireless sensor networks: a survey," *Wireless Communications*, vol. 11, no. 6, p. 6–28, 2004.

[7] N. S. a. D. W. C. Karlof, "Tinysec: A link layer security architecture for wireless sensor networks," in *In Proc. of ACM SenSys 2004*, November 2004..

[8] J. Lee, "Smart health: Concepts and status of ubiquitous health with smartphone," in *In ICT Convergence (ICTC), 2011 International Conference*, sept. 20111.

[9] J. K. E. G. a. J. B. Ramona Rednic, "Networked body sensing: Enabling real-time decisions in health and defence applications," in *In Advanced Computer Science and Information System (ICACSIS), 2011 International Conference*, 2011.

[10] M. I. M. W. a. S. S. I. Gondal, "Integrated sensing and diagnosis – the next step in real time patient health care.," in *6th IEEE/ACIS International Conference*, 2007.

[11] A. D. a. V. M. L. Cox, "Smokescreen: flexible privacy controls for presence-sharing," in *In MobiSys '07: Proceedings of the 5th international conference on Mobile systems, applications and services*, New York, NY, USA, 2007.