ISSN 2229-5518

Network Security Vulnerability and Attacks on Wireless Sensor Networks: Survey

K.M.Saravana[1], Dr. A. Kovalan[2], G.N.Basavaraj[3], Rajkumar[4]

Abstract— Wireless Sensor Networks (WSNs) are used in many applications in military, ecological and health-related areas. These applications often include the monitoring of sensitive information such as enemy movement on the battlefield or the location of personnel in a building. The cost constraints, invisible deployments will result in small sized, resource-constrained sensor nodes. While the set of challenges in sensor networks are diverse, we focus on security of Wireless Sensor Network in this paper. We propose some of the security goal for Wireless Sensor Network. Further, security being vital to the acceptance and use of sensor networks for many applications; we have made an in depth threat analysis of Wireless Sensor Network. We also propose some countermeasures against these threats in Wireless Sensor Network.

Keywords: - Wireless Sensor Networks (WSNs), Attacks, Security, Threats.

1 INTRODUCTION

Wireless sensor networks (WSN) consist of small nodes with sensing, computation, and wireless communications capabilities. Many routing, power management, and data dissemination protocols have been specifically designed for WSNs where energy awareness is an essential design issue. Routing protocols in WSNs might differ depending on the application and network architecture. A multidisciplinary research area such as wireless sensor networks, where close collaboration between users, application domain experts, hardware designers and software developers is needed to implement efficient systems. The flexibility, fault tolerance, high sensing fidelity, low cost, and rapid deployment characteristics of sensor networks create many new and exciting application areas for remote sensing. In the future, this wide range of application areas will make sensor networks an integral part of our lives. However, realization of sensor networks needs to satisfy the constraints introduced by factors such as fault tolerance, scalability, cost, hardware, topology change, environment, and power consumption. A wireless sensor network is usually a multihop wireless network consisting of spatially distributed autonomous sensing devices, measuring temperature, sound, vibration, pressure, motion or speed, pollutants, location information, utility consumption level, etc. Originally motivated by military applications, wireless sensor networks have been used in battlefield surveillance and object tracking. Early applications of networked embedded systems (or wireless sensor networks) include surveillance [1], tracking at critical facilities [2], or monitoring ecosystems [3, 4]. Current trend of networked embedded computing technology is to involve humans as part of the sensing, data collecting and computing [5, 6, 7, 10]. In this way, public and professional users are able to gather, analyze and share local information to form advanced knowledge about the surrounding physical or social world. Instead of dedicated infrastructure or special designed networks, it is more convenient and efficient to collect commonly interested information and knowledge through wireless sensor networks. The emerging applications with wireless sensor networks involve human as a part of sensing, data collecting, and computing. These applications announce the advent of a new era of ubiquitous computing and communication.

2 WSN ARCHITECTURE

In a typical WSN we see following network components as shown in fig1.1.

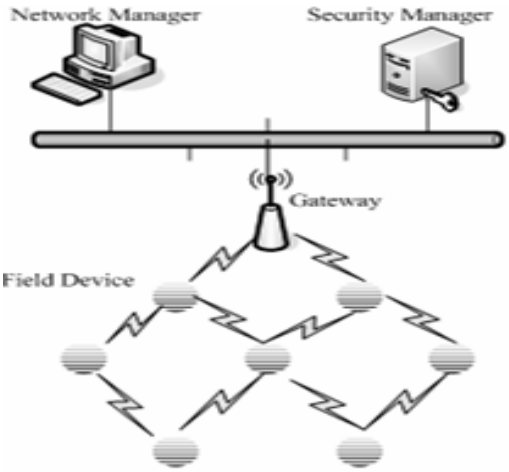

Fig1.1 WSN Architecture

Sensor motes (Field devices) – Field devices are mounted in the process and must be capable of routing packets on behalf of other devices. In most cases they characterize or control the process or process equipment.

A router is a special type of field device that does not have process sensor or control equipment and as such does not interface with

- [1]***K.M.Saravana*** *is currently pursuing Ph.D. degree, Dept. of CSE, Periyar Maniammai University, India, mailtosaravan@gmail.com*
- [2]***Dr. A. Kovalan*** *is currently working as Assistant Professor, School of CSE, Periyar Maniammai University, India, kovapmu@gmail.com*
- [3]***G.N. Basavaraj*** *is currently working as Assistant Professor, Dept. of ISE, Sambhram Institute of Technology, India, basavarajgn@gmail.com*
- [4]***Rajkumar*** *is currently working as Assistant Professor, Dept. of ISE, Sambhram Institute of Technology, India, pyage2005@gmail.com*

the process itself.
Gateway or Access points – A Gateway enables communication between Host application and field devices.

1. Network manager – A Network Manager is responsible for configuration of the network, scheduling communication between devices (i.e., configuring super frames), management of the routing tables and monitoring and reporting the health of the network.
2. Security manager – The Security Manager is responsible for the generation, storage, and management of keys.

2.1 Motivation

In publicly accessible wireless sensor networks (e.g. the above mentioned advanced metering systems), to encourage information sharing between users who may not trust each other, privacy and integrity are two important properties in information collection. Because in the civilian applications of wireless sensor networks, the data we deal with and the environments we interact with are not only about trees in the forest and animals in habitat, rather they may be critical to our properties, health and even lives, such systems will never succeed without adequate provision for data privacy and integrity. Accordingly, we will focus on two aspects of such systems, privacy preservation and integrity protection. Our objective is:

1. Protecting sensory content privacy to make the deployment of WSNs more applicable to people.
2. Enforcing integrity of collected sensory information, so users can trust it. Therefore, we focus on privacy-preserving and integrity-protecting data aggregation protocol design.

2.2 Security Requirements

The goal of security services in WSNs is to protect the information and resources from attacks and misbehavior. The security requirements in WSNs include:

1. Availability, which ensures that the desired network services are available even in the presence of denial-of-service attacks
2. Authorization, which ensures that only authorized sensors can be involved in providing information to network services
3. Authentication, which ensures that the communication from one node to another node is genuine, that is, a malicious node cannot masquerade as a trusted network node
4. Confidentiality, which ensures that a given message cannot be understood by anyone other than the desired recipients
5. Integrity, which ensures that a message sent from one node to another is not modified by malicious intermediate nodes
6. No repudiation, which denotes that a node cannot deny sending a message it has previously sent
7. Freshness, which implies that the data is recent and ensures that no adversary can replay old messages Moreover, as new sensors are deployed and old sensors fail, we suggest that forward and backward secrecy should also be considered:
8. Forward secrecy: a sensor should not be able to read any future messages after it leaves the network.
9. Backward secrecy: a joining sensor should not be able to read any previously transmitted message. The security services in WSNs are usually centered on cryptography. However, due to the constraints in WSNs, many already existing secure algorithms are not practical for use.

2.3 Challenges

Providing efficient data aggregation while preserving data privacy and integrity is a challenging problem in wireless sensor networks due to the following factors:

1. Trust management in WSN is very challenging. Users in the wireless sensor networks can be very curious to learn others' private information, and the communication is over public accessible wireless links, hence the data collection is vulnerable to attacks which threaten the privacy. Without proper protection of privacy, the communication of privacy-sensitive data over civilian wireless sensor networks is considered impractical.
2. During in-network aggregation, adversaries can easily alter the intermediate aggregation result and make the final aggregation result deviate from the true value greatly. Without protection of data integrity, the data aggregation result is not trustworthy.
3. Data collection over wireless sensor networks does not rely on dedicated infrastructure. In many cases, the number of nodes answering a query is unknown before the data aggregation is conducted.
4. Resource limited portable devices cannot afford heavy computation and communication load.
5. The requirement on accuracy of information collection (i.e., aggregated result) makes the existing randomized privacy-preserving algorithms not suitable. Besides the above mentioned factors, it is very challenging to protect privacy and integrity of data aggregation simultaneously, because usually privacy-preserving schemes disable traffic peer monitoring mechanisms, which reduces the availability of information in a neighborhood to verify data integrity.

3 ATTACK MODEL

There exist multiple potential attacks against a data aggregation protocol. Some attacks aim to disrupt the normal operation of the sensor network, such as routing attacks and DoS attacks. A good number of previous efforts [11, 12, 13] have addressed these behavior-based attacks. Sensor nodes can be compromised, and focus on the defense of the following categories of attacks in wireless sensor networks. Eavesdropping: In an eavesdropping attack, an attacker attempts to obtain private information by overhearing the transmissions over its neighboring wireless links or colluding with other nodes to uncover the secret of a certain node. Eavesdropping threatens the privacy of data held by individual nodes. Data Pollution: In a data pollution attack, an attacker tampers with the intermediate aggregation result at an aggregation node. The pur-

pose of the attack is to make the base station receive the wrong aggregation result with large deviation from the original result, and thus lead to improper or wrong decisions false reading value, because as indicated in [14] [15], the impact of such an attack is usually limited. With privacy preservation measures, the individual sensory data is hidden. However, the aggregated value of a small group of sensors must be in a reasonable range, as long as the sensory data is in a certain range. This implies that a malicious user who pollutes the individual sensory data (at a lower level in the aggregation tree) trying to introduce a large deviation can be easily detected4. Therefore, a more serious concern is the case where an aggregator close to the root of the aggregation tree is malicious or compromised.

3.1 Security Model

Encryption helps to achieve confidentiality and integrity of communication. However, encryption doesn't automatically keep privacy of individual sensory data and integrity of aggregated data. Since aggregation operation usually requires an aggregator to be aware of the content from its children, the end-to-end encryption between individual nodes and the base station will paralyze the data aggregation. On the other hand, link-level encryption itself does not keep the privacy of individual data, since the other end of the communication link is able to decrypt message and access the private data.

4 DIFFERENT ATTACKS IN WSN

4.1 Denial of Service

Denial of Service (DoS) [16], [17] is produced by the unintentional failure of nodes or malicious action. The simplest 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. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and desynchronization. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic.

4.2 Attacks on Information in transit

In a sensor network, sensors monitor the changes of specific parameters or values and report to the sink according to the requirement. While sending the report, the information in transit may be altered, spoofed, replayed again or vanished. As wireless communication is vulnerable to eavesdropping, any attacker can monitor the traffic flow and get into action to interrupt, intercept, modify or fabricate [18] packets thus, provide wrong information to the base stations or sinks. As sensor nodes typically have short range of transmission and scarce resource, an attacker with high processing power and larger communication range could attack several sensors at the transmission.

4.3 Sybil Attack

In many cases, the sensors in a wireless sensor network might need to work together to accomplish a task, hence they can use distribution of subtasks and redundancy of information. In such a situation, a node can pretend to be more than one node using the identities of other legitimate nodes. This type of attack where a node forges the identities of more than one node is the Sybil attack [19], [20]. Sybil attack is defined as a "malicious device illegitimately taking on multiple identities". It tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve. Sybil attack can be performed for attacking the distributed storage, routing mechanism, data aggregation, voting, fair resource allocation and misbehavior detection. Basically, any peer-to-peer network (especially wireless ad hoc networks) is vulnerable to Sybil attack. However, as WSNs can have some sort of base stations or gateways, this attack could be prevented using efficient protocols. Douceur [19] showed that, without a logically centralized authority, Sybil attacks are always possible except under extreme and unrealistic assumptions of resource parity and coordination among entities. However, detection of Sybil nodes in a network is not so easy. Newsome et. al. [20] used radio resource testing to detect the presence of Sybil node(s) in sensor network and showed that the probability to detect the existence of a Sybil node.

4.4 Blackhole/Sinkhole Attack

In this attack, a malicious node acts as a blackhole [21] 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. In fact, this attack can affect even the nodes those are considerably far from the base stations.

4.5 Hello Flood Attack

Hello Flood Attack is introduced in [22]. This attack uses HELLO packets as a weapon to convince the sensors in WSN. In this sort of attack an attacker with a high radio transmission (Termed as a laptop-class attacker in [22]) range and processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within a WSN. The sensors are thus persuaded that the adversary is their neighbor. As a consequence, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker.

4.6 Wormhole Attack

Wormhole attack [23] is a critical attack in which the attacker

records the packets (or bits) at one location in the network and tunnels those to another location. The tunneling or retransmitting of bits could be done selectively. Wormhole attack is a significant threat to wireless sensor networks, because; this sort of attack does not require compromising a sensor in the network rather, it could be performed even at the initial phase when the sensors start to discover the neighboring information. When a node B (for example, the base station or any other sensor) broadcasts the routing request packet, the attacker receives this packet and replays it in its neighborhood. Each neighboring node receiving this replayed packet will consider itself to be in the range of Node B, and will mark this node as its parent.

5 FUTURE TRENDS

Though significant research in WSNs and mobile computing continues, issues concerning the enablement of seamless and transparent interaction between each domain need to be resolved. A number of issues are now identified. Communication protocol issues: In order for a PDA (Personal Digital Assistants) to communicate with a sensor network, it is necessary that both PDAs and WSNs use the same communication protocol. At present, off the shelf PDAs have the Bluetooth protocol for short range communication provided. Unfortunately, studies of the Bluetooth architecture (Leopold, 2003) showed the unsuitability of such a protocol for wireless sensor networks. On the other hand, although recent advances propose a vast number of protocols tailored to WSNs, the communication compatibility between the two technologies is still an open issue. Ontology issues: Such kinds of issues arise after PDAs and sensors agree which communication protocol to use. In the context of knowledge sharing between PDAs and sensors at the application layer, they should agree with the specification of a conceptualization, also known as an ontology. Although some research propose the study of semantic techniques for wireless sensor networks (Whitehouse, 2006), a comprehensive methodology of PDA/sensor interaction is still an open issue to be addressed. Trust management issues: Requests of m-commerce-related information from sensors to PDAs and vice versa raises issues of trust management. In fact, sensors should trust the quality of service offered by the PDA protocol. On the other side, PDAs should trust sensors when, for example, product availability or machinery condition are sent to a PDA. While the latter case can be considered as an instance of internet trust management, the former case needs to consider the issue of memory capability constraints of sensors. Procedures for realizing trust management on individual sensors, for example, through intelligent agent technologies, need further research. The big "umbrella" of trust management also includes more specific issues of security. In fact, the multi-hop routing of WSNs together with the relatively simple architecture of sensors pose an inherent risk, as an attacker may only need to compromise one device to compromise the security of the entire network. This concern is amplified in applications like m-commerce where private credentials must be fully safely encoded.

6 CONCLUSION

Security is becoming a major concern for energy constrained wireless sensor network because of the broad security-critical applications of WSNs. Thus, security in WSNs has attracted a lot of attention in the recent years. The salient features of WSNs make it very challenging to design strong security protocols while still maintaining low overheads.

In this paper, we introduce sensor networks, its related security problems, threats, risks and characteristics. Network security for WSNs is still a very fruitful research direction to be further explored.

REFERENCES

[1] D. Culler, D. Estrin, and M. Srivastava, "*Overview of Sensor Networks,*" IEEE Computer,August 2004.

[2] N. Xu, S. Rangwala, K. Chintalapudi, D. Ganesan, A. Broad, R. Govindan, and D. Estrin, "*A Wireless Sensor Network for Structural Monitoring,*" Proceedings of the ACM Conference on Embedded Networked Sensor Systems, Baltimore, MD, November 2004.

[3] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson, "*Wireless Sensor Networks for Habitat Monitoring,*" WSNA'02, Atlanta, Georgia, September 2002.

[4] G. Tolle, J. Polastre, R. Szewczyk, D. Culler, N. Turner, K. Tu, S. Burgess, T. Dawson, P. Buonadonna, D. Gay, and W. Hong, "*A macroscope in the redwoods,*" in SenSys'05: Proceedings of the 3rd international conference on Embedded networked sensor systems. New York, NY, USA: ACM, 2005, pp. 51–63.

[5] A. T. Campbell, S. B. Eisenman, N. D. Lane, E. Miluzzo, and R. A. Peterson, "*People-centric urban sensing,*" in WICON '06: Proceedings of the 2nd annual international workshop on Wireless internet. New York, NY, USA: ACM, 2006, p. 18.

[6] D. Malan, T. Fulford-Jones, M. Welsh, and S. Moulton, "*Codeblue: An ad hoc sensor network infrastructure for emergency medical care,*" in International Workshop on Wearable and Implantable Body Sensor Networks, April 2004. [Online]. Available: http://www.eecs.harvard.edu/ mdw/papers/codeblue-bsn04.pdf

[7] G. Virone, A. Wood, L. Selavo, Q. Cao, L. Fang, T. Doan, Z. He, R. Stoleru, S. Lin, and J. Stankovic, "*An assisted living oriented information system based on a residential wireless sensor network*," in the 1st Distributed Diagnosis and Home Healthcare (D2H2) Conference, April 2004, pp. 95–100.

[8] T. Litman, "*London congestion pricing*," in http://www.vtpi.org/london.pdf, January 2006.

[9] B. Hull, V. Bychkovsky, Y. Zhang, K. Chen, M. Goraczko, A. K. Miu, E. Shih, H. Balakrishnan, and S. Madden, "*CarTel: A Distributed Mobile Sensor Computing System,*" in 4th ACM SenSys, Boulder, CO, November 2006.

[10] "*http://www.urban-atmospheres.net/participatoryurbanism/index.html*."

[11] Y.-C. Hu, A. Perrig, and D. B. Johnson, "*Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc NetworksNetworks*," Proceedings of INFOCOM 2003, April 2003.

[12] "*Rushing Attacks and Defense inWireless Ad Hoc Network Routing Protocols,*" ACM Workshop on Wireless Security (WiSe 2003),San Diego, CA, September 2003.

[13] I. Aad, J.-P. Hubaux, and E.W. Knightly, "*Denial of Service Resilience in Ad Hoc Networks,*" Proc. of MobiCom04, September 2004.

[14] Y. Yang, X. Wang, S. Zhu, and G. Cao, "*SDAP: A Secure Hop-by-Hop*

Data Aggregation Protocol for Sensor Networks," ACM MobiHoc, 2006.

[15] L. Hu and D. Evans, "*Secure Aggregation for Wireless Networks*," In Workshop on Security and Assurance in Ad hoc Networks, January 2003.

[16] Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, .M., Hom, R.L., and Jokerst, R.M., "*Analyzing interaction between distributed denial of service attacks and mitigation technologies*", Proc. DARPA Information Survivability Conference and Exposition, Volume 1, 22-24 April, 2003, pp. 26 – 36.

[17] Wang, B-T. and Schulzrinne, H., "*An IP traceback mechanism for reflective DoS attacks*", Canadian Conference on Electrical and Computer Engineering, Volume 2, 2-5 May 2004, pp. 901 – 904.

[18] Pfleeger, C. P. and Pfleeger, S. L., "*Security in Computing*", 3rd edition, Prentice Hall 2003.

[19] Douceur, J. "*The Sybil Attack*", 1st International Workshop on Peer-to-Peer Systems (2002).

[20] 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.

[21] Culpepper, B.J. and Tseng, H.C., "*Sinkhole intrusion indicators in DSR MANETs*", Proc. First International Conference on Broad band Networks, 2004, pp. 681 – 688.

[22] Karlof, C. and Wagner, D., "*Secure routing in wireless sensor networks: Attacks and countermeasures*", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September 2003, pp. 293-315.

[23] Hu, Y.-C., Perrig, A., and Johnson, D.B., "*Packet leashes: a defense against wormhole attacks in wireless networks*", Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE INFOCOM 2003, Vol. 3, 30 March-3 April 2003, pp. 1976 – 1986.

[24] Z.Li and G.Gong,"*A Survey on Security in Wireless Sensor Networks*" 2011.http://www.cacr.math.uwaterloo.ca/techreprorts/2008/cacr2008-20.pdf.