Wireless Sensor Network Security

Yash Sahu
Information Technology Department
Raj Kumar Goel Institute Of Technology For Women
Ghaziabad, India
yash.sahu1@gmail.com

Radha Dixit
Information Technology Department
Raj Kumar Goel Institute Of Technology For Women
Ghaziabad, India
radha.dixit123@gmail.com

Deepali Singhal
Information Technology Department
Raj Kumar Goel Institute Of Technology For Women
Ghaziabad, India
deepalisinghal@rkgitw.edu.in

Abstract: A wireless sensor network (WSN) works on the basis of sensing the situations through a number of sensors. It also helps in transmission of data. There are major security issues arising due to the growth of this technology. Since sensor networks are used in major applications like military, industries etc. which involve exchange of sensitive information therefore privacy preservation is an important issue in wireless sensor network. Due to limited resources the development of effective security solution is difficult. This research paper mainly concerns with problems associated in developing security protocols for wireless sensor networks, their requirements, different types of attacks on sensor networks and brief overview of existing security protocols.

Keywords: Wireless sensor network (WSN), Routing, Security, Attack

I. INTRODUCTION

We use the term sensor network to refer to a heterogeneous system combining tiny sensors and actuators with general purpose computing elements. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. Realization of sensor network applications requires wireless ad hoc networking techniques. However protocols and algorithms proposed for traditional ad hoc networks are not well suited due to the unique features and application requirements of sensor networks. Because of its unique features, sensor networks are used in wide range of applications in areas like health, military, home and commercial industries in our day to day life.

As WSN is mostly used for gathering application specific information from the surrounding environment, it is highly essential to protect the sensitive data from unauthorized access. WSNs are vulnerable to security attacks due to the broadcast nature of radio transmission. Sensor nodes may also be physically captured or destroyed by the enemies. The uses of sensor network in various applications emphasis on secure routing. Various protocols are proposed for routing and data gathering but none of them are designed with security as a goal. The resource limitation of sensor networks poses great challenges for security. As sensor nodes are with very limited computing power, it is difficult to provide security in WSN using public-key cryptography. Therefore most of the proposed security solutions for WSN are based on symmetric key cryptography. In this paper we have reviewed possible attacks on WSN in general as well as attacks on specific WSN data gathering protocols.

II. OBSTACLE IN DEVELOPING SECURITY PROTOCOLS FOR SENSOR NETWORKS

A wireless sensor network has many resource constraints as compared to the traditional computer networks. Due to these resource constraints it is difficult to directly employ the existing security approaches to the area of wireless sensor networks. We have some protocols and algorithms which do a satisfactory job of securing internet communication. However these protocols and algorithms are too heavy weight for use in sensor network. They are having very high communication overheads and they are not designed to run on computationally constrained devices. They will also increase power consumption. So there is a need for new more energy efficient cryptographic algorithms and protocols.

Let us discuss various obstacles in developing security protocol for sensor networks.

A. Power Consumption Limitation:

The wireless sensor node, being a micro-electronic device, can only be equipped with a limited power source of battery ratings of (<0.5 Ah, 1.2 V). Energy is the biggest constraint to wireless sensor capabilities. Once sensor nodes are deployed in a sensor network, they cannot be easily replaced (high operating cost) or recharged (high cost of sensors).When implementing a cryptographic function or protocol within a sensor node, the energy impact of the added security code must be considered. When adding security to a sensor node, we are interested in the impact that security has on the lifespan of a sensor (i.e., its battery life). The extra power consumed by sensor nodes due to security is related to the processing required for security functions (e.g., encryption, decryption, signing data, verifying signatures), the energy required to transmit the security related data or overhead (e.g., initialization vectors needed for encryption/decryption), and the energy required to store security parameters in a secure manner (e.g., cryptographic

ISBN: 9788175157538

key storage).The limited Energy supplies creates problem for security.

These power constraints make it impractical to use most current secure algorithms, since they are designed for powerful processors.

In other mobile and ad hoc networks, power consumption has been an important design factor, but not the primary consideration, simply because power resources can be replaced by the user. The emphasis is more on Quality of Service provisioning than the power efficiency.

But, in sensor networks, power efficiency is an important performance so; security protocols can be designed by appropriately trading off other performance metrics with power efficiency.

B. Memory and Storage Limitation:

A sensor is a tiny device with only a small amount of memory and storage space for the code. In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm. For example, smart dust node (Refer Table No. 1) sensor type has an 8-bit, 4MHZ CPU only with only 8 Kbytes Instruction flash, 512 byte RAM and 512 byte EPROM. With such a limitation, the software built for the sensor must also be quite small.

So it is clear that sensor networks differ from other distributed system in a important ways. These devices have very little computational power; even efficient public key cryptography and fast symmetric ciphers must be used with care. There is a considerable pressure to ensure that security protocol use a minimal amount of limited RAM. Additionally communication bandwidth is extremely dear. Each bit transmitted consumes about as much power as executing 800-1000 instructions and any message expansion caused by security mechanism comes at significant cost. Energy is scarcest resource of all.

Table 1: Characteristic of smart dust node

Sr.no	Operational parameters	Values
1.	CPU	8 bit, 4 MHz, 8 Kbytes Instruction flash 512 Byte RAM 512 Byte EPROM
2.	Communication	916 MHz Radio
3.	Bandwidth	10 Kbps
4.	Operating System	Tiny OS
5.	Operating System Code Space	3500 bytes
6.	Available Code space	4500 e s

C. Unreliable Communication:

Certainly, unreliable communication is another threat to sensor security. Normally the packet-based routing of the sensor network is connectionless and thus inherently unreliable. Packets may get damaged due to channel errors or dropped at highly congested nodes. The result is lost or missing packets. Furthermore, the unreliable wireless communication channel also results in damaged packets. If the protocol lacks the appropriate error handling it is possible to lose critical security packets, for example, a cryptographic key.

D. Conflicts:

Even if the channel is reliable, the communication may still be unreliable due to the broadcast nature of the wireless sensor network. If packets meet in the middle of transfer, conflicts will occur and the transfer itself will fail. In a crowded (high density) sensor network, this can be a major problem.

E. Latency:

The multi-hop routing, network congestion, and node processing can lead to the latency of the network, thus make it difficult to achieve the synchronization among sensor nodes. The synchronization issues can be critical to sensor security where the security mechanism relies on critical event reports and cryptographic key distribution.

F. Unattended operation:

Depending on the function of the particular sensor network, the sensor nodes may be left unattended for long periods of time. Due to remote management of a sensor network makes it becomes virtually impossible to detect physical tampering (i.e., through tamper-proof seals) and physical maintenance issues (e.g., battery replacement) of sensor nodes.

G. No central management point:

A sensor network is a distributed network without a central management point. This increases the vitality of the sensor network. But at the same time it makes the network organization difficult, inefficient, and fragile.

III. SECURITY ATTACKS

Because sensor network uses wireless communication, they are vulnerable to attacks, which are more difficult to launch in the wired domain. Many wired network benefit from their inherent physical security properties. It is unlikely that an adversary will dig up the Internet Backbone and splice in to line. However wireless communication is difficult to protect; they are by nature a broadcast medium. In broadcast medium adversaries can easily eavesdrop on, intercept, inject and alter transmitted data. Sensor network are also vulnerable to resource consumption attacks. Adversaries can repeatedly send packets to drain the node batteries and waste network bandwidth. Adversaries can also insert false data or Change routing behaviour.

Attacks can be performed in a variety of ways, most notable as denial of service attacks, Sybil Attacks, attacks against privacy, physical attacks which are discussed in the next paragraph.

A. Spoofed, altered, or replayed routing information:

This is the most common direct attack against a routing protocol. This attack targets the routing information

ISBN: 9788175157538

exchanged between the nodes. Adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, and increase end-to-end latency. The standard solution for this attack is authentication. i.e., routers will only accept routing information from valid routers.

B. Selective forwarding attack:

Multi-hop mode of communication is commonly preferred in wireless sensor network data gathering protocols. Multi-hop networks assume that participating nodes will faithfully forward and receive messages. However a malicious node may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. This attack can be detected if packet sequence numbers are checked properly and continuously in a conjunction free network. Addition of data packet sequence number in packet header can reduce this attack.

C. Sinkhole attack:

By sinkhole attack, the adversary tries to attract nearly all the traffic from a particular area through a compromised node. A compromised node which is placed at the centre of some area creates a large “sphere of influence”, attracting all traffic destined for a base station from the sensor nodes. The attacker targets a place to create sinkhole where it can attract the most traffic, possibly closer to the base station so that the malicious node could be perceived as a base station. The main reason for the sensor networks susceptible to sinkhole attacks is due to their specialized communication pattern. It may be extremely difficult for an adversary to launch such an attack in a network where every pair of neighbouring nodes uses a unique key to initialize frequency hopping or spread spectrum communication. Sinkholes are difficult to defend in protocols that use advertised information such as remaining energy or an estimate of end-to-end reliability to construct a routing topology because this information is hard to verify.

D. Sybil attack:

Most protocols assume that nodes have a single unique identity in the network. In a Sybil attack, an attacker can appear to be in multiple places at the same time. This can be convincing by creating fake identities of nodes located at the edge of communication range. Multiple identities can be occupied within the sensor network either by fabricating or stealing the identities of legitimate nodes. Sybil attacks can pose a significant threat to geographic routing protocols. Location aware routing often requires nodes to exchange coordinate information with their neighbours to construct the network. So it expects nodes to be present with a single set of coordinates, but by using the Sybil attack an adversary can ‘‘be in more than one place at once’’. Since identity fraud leads to the Sybil attack, proper authentication can defend it.

E. *Wormhole attack*:

In this attack an adversary could convince nodes who would normally be multiple hops from a base station that they are only one or two hops away via the wormhole. The simplest case of this attack is to have a malicious node forwarding data between two legitimate nodes. Wormholes often convince distant nodes that they are neighbours, leading to quick exhaustion of their energy resources. An adversary situated close to a base station may be able to completely disrupt routing by creating a well-placed wormhole. Wormholes are effective even if routing information is authenticated or encrypted. This attack can be launched by insiders and outsiders. This can create a sinkhole since the adversary on the other side of the wormhole can artificially provide a high quality route to the base station, potentially all traffic in the surrounding area will be drawn through her if alternate routes are significantly less attractive. When this attack is coupled with selective forwarding and the Sybil attack it is very difficult to detect. More generally, wormholes can be used to exploit routing race conditions. A routing race condition typically arises when a node takes some action based on the first instance of a message it receives and subsequently ignores later instances of that message. The goal of this attack is to undermine cryptography protection and to confuse the sensor’s network protocols. We can prevent this by avoid routing race conditions. The solution requires clock synchronization and accurate location verification, which may limit its applicability to WSNs.

IV. RELATED WORK AND SECURITY SOLUTIONS IN WSN

In the recent years, wireless sensor network security has been able to attract the attentions of a number of researchers around the world. In view of resource limitation on sensor nodes, size and density of the networks, unknown topology prior to deployment, and high risk of physical attacks to unattended sensors, it becomes very challenging task to apply security schemes in wireless sensor networks.

While much research has focused on making these networks feasible and useful, security has received little attention.

Researchers have been trying to resolve security issues.

Most of the existing security mechanisms require intensive computation and memory. Many security mechanisms require repeated transmission/communication between the sensor nodes which are further drawn in their resources. In this section, we review some of the popular security solutions and combat some of the threats to the sensor networks.

A. SPINS

Security protocols for sensor networks (SPIN) was proposed by Adrian Perrig *et al* in which security building blocks optimized for resource constrained environments and wireless communication. SPINs has two secure building blocks:

- sensor network encryption protocol (SNEP) and
- µTESLA. SNEP provides data confidentiality, two-party data authentication, and data freshness. µTESLA provides authenticated broadcast for severely resource-constrained environments.

ISBN: 9788175157538

SNEP uses encryption to achieve confidentiality and message authentication code (MAC) to achieve two-party authentication and data integrity. Since sending data over the RF channel requires more energy, all cryptographic primitives such as encryption, MAC, hash, random number generator, are constructed out of a single block cipher for code reuse. This, along with the symmetric cryptographic primitives used reduces the overhead on the resource constrained sensor network. SNEP provides number of advantages such as low communication overhead, semantic security which prevents eavesdroppers from inferring the message content from the encrypted message, data authentication, replay protection, and message freshness.

µTesla is a new protocol which provides authenticated broadcast for severely resource-constrained environments.

In a broadcast medium such as sensor network, asymmetric digital signatures are impractical for the authentication, as they require long signatures with high communication overhead. µTesla protocols provide efficient authenticated broadcast and achieves asymmetric cryptography by delaying the disclosure of the symmetric keys. µTesla constructs authenticated broadcast from symmetric primitives, but introduces asymmetry with delayed key disclosure and one-way function key chains. µTESLA solves the following inadequacies of TESLA in sensor networks:

- TESLA authenticates the initial packet with a digital signature, which is too expensive for our sensor nodes. µTESLA uses only symmetric mechanisms.
- Disclosing a key in each packet requires too much energy for sending and receiving. µTESLA discloses the key once per epoch.
- It is expensive to store a one-way key chain in a sensor node. µTESLA restricts the number of authenticated senders.

B. TINYSEC

TinySec is link layer security architecture for wireless network, which was designed by Karlof *et al*. It provides similar services as of SNEP, including authentication, message integrity, confidentiality and replay protection. It is a lightweight, generic security package that can be integrated into sensor network applications. A major difference between TinySec and SNEP is that there are no counters used in TinySec.

TinySec provides the basic security properties of message authentication and integrity using MAC, message confidentiality through encryption, semantic security through an Initialization Vector and replay protection.

TinySec supports two different security options: authenticated encryption (TinySec- AE) and authentication only (TinySec-Auth). For authenticated encryption (TinySec-AE), TinySec uses cipher block chaining (CBC) mode and encrypts the data payload and authenticates the packet with a MAC. The MAC is computed over the encrypted data and the packet header. In authentication only mode (TinySec-Auth), TinySec authenticates the entire packet with a MAC, but the data payload is not encrypted.

C. LEAP

Localized encryption and authentication protocol (LEAP)

Protocol is a key management protocol for sensor networks. It is designed to support in-network processing and secure communications in sensor networks. LEAP provides the basic security services such as confidentiality and authentication. In addition, LEAP is to meet several security and performance requirements that are considerably more challenging to sensor networks. Design of the LEAP protocol is motivated by the observation that different types of messages exchanged between sensor nodes have different security requirements. LEAP has the following properties:

- LEAP supports the establishment of four types of keys for each sensor node – an individual key shared with the base station, a pairwise key shared with another sensor node, a cluster key shared with multiple neighbouring nodes, and a group key that is shared by all the nodes in the network. The protocol used for establishing and updating these keys is communication and energy efficient, and minimizes the involvement of the base station.
- LEAP includes an efficient protocol for inter-node local broadcast authentication based on the use of one-way key chains.
- Key sharing approach of LEAP supports source authentication without precluding in-network processing and passive participation. It restricts the security impact of a node compromise to the immediate network neighbourhood of the compromised node.

V. 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 have introduced some security issues, threats, and attacks in WSNs and some of the solutions. Network security for WSNs is still a very fruitful research direction to be further explored.

ACKNOWLEDGEMENT

This research would not have taken shape, without the guidance provided by Ms.Deepali Singhal, who helped in our project and resolved all the technical as well as other problems related to the project and, for always providing us with a helping hand whenever we faced any bottlenecks, inspite of being quite busy with their hectic schedules.

ISBN: 9788175157538

Above all we wish to express our heartfelt gratitude to HOD, Ms.Kadambari Agarwal whose support has greatly boosted our self-confidence and will go a long way on helping us to reach further milestones and greater heights.

REFERENCES

[1] Lin, R., Wang, Z. & Sun, Y., (2004) "Wireless Sensor Networks Solutions for Real Time Monitoring of Nuclear Power Plant in", The Proceedings of the 5' World Congress on intelligent Control and Automation, Hangzhou, P.R. China.

[2] Römer, K., Mattern, F. & Zurich, E., (2004) "The Design Space of Wireless Sensor Networks", IEEE Wireless Communications.

[3] Yoneki, E. & Bacon, J., (2005) "A survey of Wireless Sensor Network technologies: research trends and middleware's role", technical report. http://www.cl.cam.ac.uk/TechReports, ISSN 1476-2986.

[4] Kaplantzis, S., (2006) "Security Models for Wireless Sensor Networks",http://members.iinet.com.au/~souvla/transferfinal- rev.pdf

[5] Sohrabi, K., Gao, J., Ailawadhi, V., and Pottie, G. J., (2000) "Protocols for Self- Organization of a Wireless Sensor Network", IEEE Personal Communications, pp. 16-27.

[6] Woo, A. and Culler, D., (2001) "A Transmission Control Scheme for Media Access in Sensor Networks", Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 2001), Rome, Italy.

[7] Shih, E., Cho, S., Ickes, N., Min, R., Sinha, A., Wang, A. & Chandrakasan, A., (2001) "Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks", Proceedings of the 7th Annual International Conference on Mobile Computing and Networking, Rome, Italy, pp. 272-287.

[8] Shen, C., Srisatjapornphat, C., and Jaikaeo, C., (2001) "Sensor Information Networking Architecture and Applications", IEEE Pers. Communication, pp. 52–59.

[9] Committee on National Security Systems (CNSS), (2006) National Information Assurance Glossary, NSTISSI,No. 4009. Journal of Theoretical and Applied Information Technology © 2005 - 2010JATIT. All rights reserved. www.jatit.org 26 http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

[10] Wood, A. and Stankovic, J. A., (2002) "Denial of Service in Sensor Networks", IEEE Computer, 35(10):54-62, pp. 54-62.

[11] Walters, J. P., Liang, Z., Shi, W., and Chaudhary, V., (2007) "Wireless sensor network security - a survey", Security in Distributed, Grid, Mobile, and Pervasive Computing, Auerbach Publications, CRC Press.

[12] Stallings, W., (2000) Cryptography and Network Security Principles and Practice, Cryptography Book, 2nd Edition, Prentice- Hall, 0-13-869017-0.

[13] Karlof, C., and Wagner, D., (2003) "Secure Routing in Sensor Networks: Attacks and Countermeasures", *SNPA*, pp. 1-15.

[14] Saxena, M., (2007) "Security in Wireless Sensor Networks – A Layer based classification", Technical Report [CERIASTR 2007-04], *Center for Education and Research in Information Assurance and Security - CERIAS*, Purdue University. pages.cs.wisc.edu/~msaxena/papers/2007-04-cerias.pdf

[15] Fernandes, L. L., (2007) "Introduction to Wireless Sensor Networks Report", University of Trento. http://dit.unitn.it/~fernand/downloads/iwsn.pdf

ISBN: 9788175157538