Light Weight Security Protocol for Wireless Sensor Network’s (WSN)

Aarti Arjun Andhale
PG Student
Computer Engineering Department
MITCOE,Pune 38

Prof. B.N. Jagdale
Assistant Professor
Information Technology Department
MITCOE,Pue 38

Abstract -Security is one of the most important requirement of Wireless Sensor Network’s(WSN) applications. The main motive of our work is to minimize attacks without causing any impact on transferring data. To minimize attacks we have to develop Light Weight Security Protocol for Wireless Sensor Network's(WSN).It typically deals with protecting communication among network devices, as well as contrasting logical and physical attacks at different layers.

Index Terms - Wireless sensor networks,Cryptography

1. Introduction

Wireless sensor networks consists of distributed sensors to monitor physical and environmental conditions such as temperature, sound, vibration,pressure, motion or pollutants and to cooperatively pass their data through the network to a main location. The main characteristics of a WSN include: i)power consumption constrains for nodes using batteries or energy harvesting.ii)Ability to cope with node failures. iii)Mobility of nodes iv)Ease of use.

Applications of Wireless Sensor Networks are divided into following categories: i) Military Applications ii)Environmental Applications iii)Health applications iv)Home and other commercial applications. Wireless sensor network security has been focused on the security services that provide authentication,confidentiality,integrity,availability. Security protocols needs to satisfy all these security services to provide good results.

A sensor network is capable of sensing, processing and communicating which helps the base station or command node to observe and react according to the condition in a particular environment (physical, battle field, biological) [1].There are two types of security goals of WSN: i) Primary goals ii)Secondary goals. The primary goals are known as standard security goals such as Confidentiality, Integrity, and Authentication. The secondary goals are Data Freshness, Time Synchronization and Secure Localization. There are many Symmetric Cryptography techniques that can be used in WSNs. For example, SPINS [2] used RC5 [3] as the block cipher. TinySec [4] used Skipjack [5] as the default block cipher.

Neighborhood Based Security Protocol is used to provide authentication in Wireless Sensor Network’s(WSN). NEKAP [6], a design of link layer key agreement protocol for sensor networks. NEKAP can provide the Confidentiality but sometimes this protocol fails to provide authentication. For Light Weight Security Protocol sometimes we have to use Symmetric and Asymmetric Cryptography techniques. Cryptography is a standard method to provide security in Wireless Sensor Network’s(WSN).

Using Cryptographic techniques we can increase the lifetime of the network. A Lots of work has been done to proposed the secure data aggregation protocol. Only some of them focused on Data Integrity.

2. Security Services or Requirements

Confidentiality: Confidentiality aims to prevent unauthorized reading of information. This service ensures that the exchanged data is kept secret from any unauthorized user over the network. It is usually achieved using symmetric encryption technique.

Integrity: Information has integrity if unauthorized writing is prohibited.It protects data from unauthorized or accidental modi_cation through the use of firewalls, cryptography, and intrusion detection tools.Data should not be changed during the transmission from source to destination.

Availability: Data availability has become a fundamental issue in information security.It involves sound disaster recovery planning procedures based on an accepted business continuity plan

3. Security issues in Wireless Sensor Networks

Traditional security mechanisms normally require high processing capability, and large memory and storage requirements. Such resources are not available in nodes in a wireless sensor network. As a result of these constraints, designing effective security mechanisms is more difficult than for a wired network. Examples of these constraints include:

(a)**Small memory:** Wireless sensor node has very limited memory with small storage capacity. As a result, any security mechanism to be designed and run within a sensor network will have limitations and not be as robust as one for a wired network.

(b) **Reduced energy levels:** Designing security mechanisms for wireless sensor networks must consider the reduced energy levels that are implicit with sensor nodes. When a sensor node is deployed, its energy source is usually a battery so it is critical to design security features that are not memory or power intensive in order to prevent the battery life being exhausted quickly. However, security features will consume extra energy that that required for normal operation, for example cryptographic techniques, and this may be detrimental to the sensor node's time to live.

(c) **Communication problems:** There is an inherent problem with wireless communication in that data can get intercepted, lost and is generally prone to attack. Data packets will be damaged or lost because of in Wireless Sensor Networks lots of data transmitted and received between sensor nodes and it results in heavy network traffic.

(d) **Physical security:** An attacker can potentially capture or damage a node. Sensor nodes are generally small devices that are not very robust.

3.1Threats and Issues in Wireless Sensor Networks

Wireless networks are usually more vulnerable to various security threats.

3.1.1 Denial of Service (DoS) attack:

It occurs 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[7][8]. 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.

3.1.2 Wormhole Attack

A wormhole attack is one whereby an attacker tunnels messages received in one part of the network over a low latency link and replays them in a different part. Wormholes may also be used simply to convince two distant nodes that they are neighbours by relaying packets between the two of them[9].

3.1.3 Sybil Attack

Idea: a single node pretends to be present in different parts of the network. a single node presents multiple identities to other nodes in the network. The Sybil attack can significantly reduce the effectiveness of fault-tolerant schemes such as distributed storage, disparity and multipath routing, and topology maintenance Replicas, storage partitions, or routes believed to be using disjoint nodes could inactuality be using a single adversary presenting multiple identities.

A Sybil attack is one in which a sensor node mimics the identity of more than one other legitimate nodes [10,11]. All peer-to-peer networks are susceptible to a sybil attack. However, the detection of sybil nodes is difficult [11].

4. Types of Cryptographic Techniques

Cryptography is not only protects data from theft or alteration, but can also be used for user authentication.Three types of Cryptographic schemes typically used to accomplish these goals: Secret key Cryptography, Public key Cryptography and hash functions.

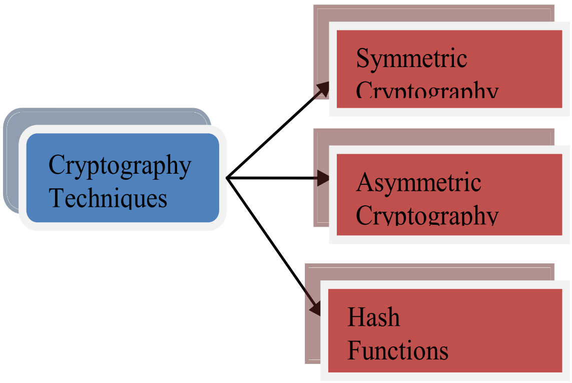


Figure 1: Cryptographic Techniques

A. Symmetric Cryptography or Secret key Cryptography

If both sender and receiver use the same key,the system is referred to as symmetric, single key, secret key or conventional encryption. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.

If someone can discover the key and knows the algorithm , all communication using this key is readable. Two types of symmetric ciphers are used: block ciphers that work on blocks of a specific length and stream ciphers that work bitwise on the data. A steam cipher can be seen as a block cipher with a block length of 1 bit.

B. Public key Cryptography

Public key algorithms rely on one key for encryption and a different but related key for decryption. If Bob wishes to to send a confidential message to Alice, Bob encrypts the message using Alice's public key.

When Alice receives the message, she decrypts it using her private key. No other recipient can decrypt the message because only Alice knows Alice's private key.

C. Hash Functions

A hash value h is generated by a function H of the form

$$h=H(M)$$

where M is a variable length message and H(M) is the fixed length hash value. The purpose of the hash function is to produce a "fingerprint" of a file, message, or other block of data.

One of the simplest hash functions is the bit by bit exclusive-OR (XOR) of every block. This can be expressed as follows:

$$Ci= bi1\ XOR\ bi2\ XOR…….. XOR\ bim$$

5. Light Weight Security Protocols for WSNs

We present various energy efficient architectures that can be employed in physical, data link, network, and middleware layers of the OSI communication model. In this section, we survey some of more and less common security solutions for Wireless Sensor Networks.

5.1 *LEAP/LEAP+: Localized Encryption and Authentication Protocol*

LEAP was designed as a key management protocol to provide secure communication in WSNs. LEAP [12] and LEAP+ [13] are lightweight, energy efficient security protocols for large scale sensor networks. They provide confidentiality and authentication services. The RAM usage and energy costs depend on the number of nodes in a network. The implementation of LEAP requires about 17.8 KB of program space. Due to various security requirements for different types of messages four types of keys for each network node are established: an individual key shared with a base station, a pairwise key shared with another node, a cluster key shared with a group of neighboring nodes, and a group key globally shared with all nodes in a network.

5.2 LSec: Lightweight Security Protocol

It is the energy and memory efficient technique that assumes grouping network nodes into clusters. The Lightweight Security Protocol for distributed wireless sensor network (LSec) is described in [14]. LSec provides following security capabilities: authentication, authorization, confidentiality of data, and protection against intrusions and anomalies.Both symmetric and asymmetric security schemes are used.

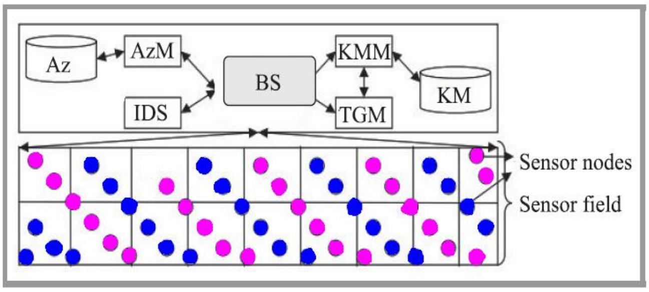


Figure 2: LSec system architecture[14].

The LSec architecture consists of the following modules:

KMM key management module: stores public andshared secret key of each node with a base station(BS) to the database(KM),

• **TGM token generator module**: generates the tokens for the requesters,

• **AzM authorization module:** checks whether a particular node is allowed to communicate with other node or a group ofnodes,

• **IDS intrusion detection**; cluster heads send alert messages to IDS (lightweight mobile agents are installed in cluster heads).

LSec combines the features of trusted server scheme and self enforcing security scheme. LSec is highly scalable and memory efficient – it introduces only 74.125 bytes of transmission and reception cost per connection. It provides stronger security and has the advantage of simple secure defense mechanism against compromised nodes. LSec is employed in the middleware layer of the communication model. It is scalable and memory efficient solution.

It is assumed that the base station is the trusted party that never is compromised. Only the base station has an access to the public keys of all nodes in the network, and communicating nodes know each other's public keys only during the time of connection establishment. An asymmetric scheme is used for sharing ephemeral secret key between communicating nodes. For every session, new random secret key is used. Each node has to store six keys (public key of node, private key of node, public key of BS, group key, public key of other node, session key). 72 bytes of memory are needed to store these keys.

5.3 SPINS: Security Protocol for Sensor Network

It consists of two secure building blocks,i.e., Secure Network Encryption Protocol (SNEP) and micro version of Timed Efficient Stream Loss-tolerant Authentication (µTESLA). SNEP is used to provide confidentiality using encryption, and authentication, integrity and freshness of data using Message Authentication Code (MAC). The SPINS protocol developed by A. Perrig *et al*, is described in [15]. In Message Authentication Code (MAC) approach all cryptographic primitives are constructed from a single block cipher for code reuse. Thus, the communication overhead is limited.

µTESLA is used for broadcasted data authentication. µTESLA requires that the base station and network nodes are loosely time-synchronized, and each node knows an upper bound on the maximum synchronization error. µTESLA provides stronger security for networks with constrained resources because of it generates authenticated broadcast message using symmetric key, and introduces asymmetric cryptography by delaying the disclosure of the symmetric keys.

The implementation of SPINS requires about 220 bytes of RAM and 1580 to 2674 bytes of program space. An increase of energy consumption for security is about 20%.

5.4 *TinySec: Link Layer Security Architecture for Wireless Sensor Networks*

The main problem with SPINS is that it has not been yet fully specified and implemented. TinySec is a link layer security architecture designed by Ch. Karlof *et al.*, and presented in [16]. Similarly to the SNEP protocol, it provides authentication, message integrity and confidentiality services.

The message authentication and integrity is provided using MAC, message confidentiality using encryption. Two security modes are possible – authentication only and authenticated encryption. In case of the first mode, the entire packet is authenticated using MAC, but the payload data is not encrypted. In case of the second mode, the payload data is encrypted and then authenticated with a MAC. Any keying mechanisms can be employed(single network-wide keys, per-link keys, group keys, etc.).

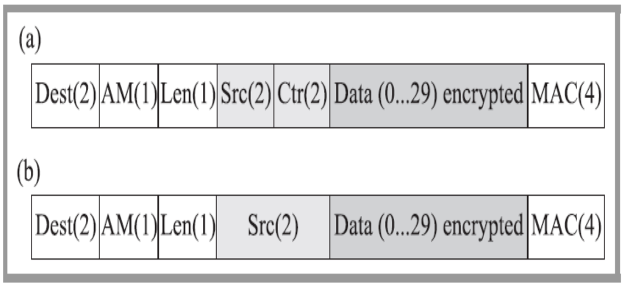
TinySec is designed as a lightweight, energy efficient security package. It can be easily integrated into any WSN application. The implementation of TinySec requires about 728 bytes of RAM and 7146 bytes of program space. Anincrease of energy consumption depends on the mode andnetwork technology, and is about 3% to 9,1% higher in compare to a normal TinyOS packet transmission.

5.5 *LLSP: The Link-Layer Protocol*

A Link-Layer Protocol (LLSP) was designed by L. E. Ligh-foot *et. al.*, and is described in [17]. LLSP guarantees various security requirements but focuses on three security services: message authentication, message confidentiality, and replay protection. The aim was to develop a protocol with less energy requirements than Tiny-Sec.

AES-CBC mode of operation as the data encryption scheme is implemented in LLSP. The unique design of AES-CBC provides semantic security, i.e., encrypting the same plaintext twice will produce two different ciphertexts. A synchronous 4-byte counter between the sender and receiver pair is proposed to replay protection. Feedback Shift Register (FSR) is used to update this counter. The LLSP packet format is based on the TinySEC one. The LLSP security protocol reduces the energy usage without decreasing the security level.

The LLSP secure protocol was evaluated via simulation and compared with the TinySec protocol.



(a)

Dest(2)	AM(1)	Len(1)	Src(2)	Ctr(2)	Data (0...29) encrypted	MAC(4)

(b)

Dest(2)	AM(1)	Len(1)	Src(2)	Data (0...29) encrypted	MAC(4)

Figure 3: Packet format in TinySec (a) and in LLSP (b)

Both applications were executed in the TOSSIM simulator(docs.tinyos.net/index.php/TOSSIM). The results are presented in [17]. From these results we can see that similar to most security protocols, the computational and energy costs increase for each packet transmission. It is concerned with extra computations and the larger packet size due to the security overhead. However, the authors of the LLSP protocol claim that using their solution the energy consumption is about 15% smaller than for TinySec, and latency reduction is about 3%.

5.6 *HASF: The Hybrid Adaptive Security Framework*

Hybrid Adaptive Security Framework (HASF) is a security architecture developed by T. Shon *et al.*, and described in [18]. In HASF, security functions are embedded to the network layer and the link layer (MAC) of the OSI model separately. The main idea is to provide hybrid adaptive security suite to each packet transmitted in a given WSN. This framework provides security capabilities with less extra energy usage than TinySec. The Hybrid Adaptive Security Suite (HASS) proposed in HASF is almost the same as the security suite proposed for IEEE 802.15.4.

The differences to commonly used architectures in HASS are as follows:

– *null* security is not provided,

– security suite is dynamically applied to MAC frame due to a type of a given WSN.

Three network characteristics are distinguished: *public*, *commercial*, *private*. Various security capabilities are provided to these groups of network. None confidentiality is guaranteed for public networks, more security capabilities are provided in commercial networks, and the strongest security is provided in private networks. All data are divided into control and application. *Control data* means a message or signal to manage the network operation. *Application data* means a kind of data concerned with WSN services. The attributes of these data are: periodic, urgent-periodic,on-demand, event-driven.

5.7 Security Protocol Based on NOVSF

The cluster-based security protocol proposed in [19] uses a symmetric cryptography algorithm to guarantee security.To reduce the drawbacks of a symmetric cryptography andprovide complete security, it employs the code-hopping technique using the Non-Orthogonal Variable SpreadingFactor (NOVSF) codes. The NOVSF is an implementation of the non-blocking transmission of CDMA. In NOVSF codes, each OVSF code has 64 time slots, and any number of these time slots can be assigned to a channel. In NOVSF, the data blocks are assigned to time slots using different permutations in every session,

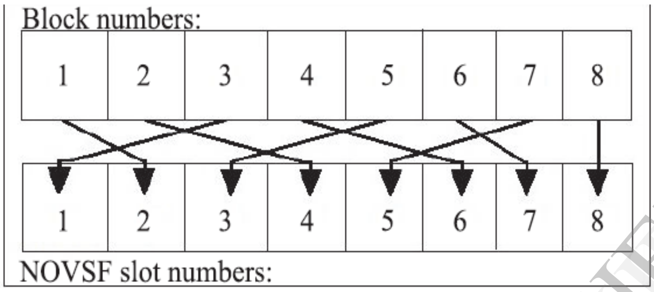


Figure 4: Code-hopping technique.

Hence, the blocks of data are finally mixed, and such reordering method supports security. The algorithm operates as follows. First,it is assumed that all network nodes are grouped into disjoint and mostly non-overlapping clusters. As a result, a hierarchical communication structure consisting of a base station, cluster heads and the lowest level formed by members of clusters is obtained. Secondly, the following steps of the algorithm are performed:

***Step 1*:** A base station periodically broadcasts the session key.

***Step 2*:** Sensor nodes generate their cryptographic keys.

***Step 3*:** The encrypted data are transmitted from sensor nodes to cluster heads using NOVSF code-hopping technique.

***Step 4*:** Each cluster head appends its identifier number(ID) to this data and then forwards such data to the higher level cluster heads.

Step 5: The message is decrypted and authenticated by the base station.

The transmission between nodes and cluster heads is encrypted. Based on periodically changed user specific session keys and NOVSF codes assigned to eachnode the authentication of messages is performed. Moreover, changing encryption keys from time to time guarantees data freshness in a network. The CBC-MAC protocol is used to provide data integrity. The total memory space for applied cryptographic primitives are about 2 KB. Hence, applying the NOVSF code-hopping technique increases security capabilities without requiring additional energy.

6. Conclusion

We briefly discussed the security requirements of WSNs and Threats and Issues in Wireless Sensor Networks, Types of Cryptographic Techniques, Light Weight Security Protocols for WSNs, Secure Energy Efficient Routing Protocols. The paper provides a short overview of some representative energy efficient security techniques.

REFERENCES

[1] K. Sohraby, D. Minoli, and T. Znati, "Wireless sensor networks:technology, protocols and applications," *New Jersey: John Wiley*, pp.38-71, 2007.
[2] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: Security Protocols for Sensor Networks", *ACM Wireless Networks*, 8(5):521-
534, Sept. 2002.
[3] R. Rivest, "The RC5 encryption algorithm", *Proc. 1st Workshop on Fast*
Software Encryption, 1995, pp. 86 - 96.
[4] C. Karlof, N. Sastry, and D.Wagner, "TinySec: a link layer security architecture for wireless sensor networks", *Proceedings of the 2nd international conference on Embedded networked sensor systems*, Baltimore, MD, USA, pp. 162 - 175.
[5] Skipjack and KEA algorithm specifications. http://csrc.nist.gov/encryption/skipjack/skipjack.pdf, NIST, 1998.
[6] De Oliveira S., Hao Chi Wong and Nogueira J.M., "NEKAP: Intruder
Resilient and Energy Efficient Key Establishment in Sensor Networks",*International Conference Computer Communication and Networks, 2007(ICCCN '07),* Honolulu, Hawaii, USA, 2007.
[7] Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.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.
[8] 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.
[9] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Wormhole detection in wireless ad hoc networks," Tech. Rep. TR01-384, Department of Computer Science, Rice University, June 2002.
[10] Douceur, J. "The Sybil Attack", 1st International Workshop on Peer-to-Peer Systems (2002).

[11] 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.

[12] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks", in *Proc. 10th ACM Conf. Comp. Commun. Secur. CCS 2003*, Washington, DC,USA, 2003, pp. 62–72.

[13] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks", *ACM Trans. Sensor Netw. TOSN*, vol. 2, no. 4, pp. 500–528, 2006.

[14] R. A. Shaikh, S. Lee, M. A. U. Khan, and Y. J. Song, "LSec:lightweight security protocol for distributed wireless sensor network", *Lecture Notes in Computer Science*, vol. 4217, 2006.

[15] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. Culler, "SPINS:
security protocols for sensor networks", *Wirel. Netw.*, vol. 8, no. 5,pp. 521–534, 2002.

[16] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks", in *Proc. 2nd Int. Conf.Embedded Networked Sensor Sys.*, Baltimore, MD, USA, 2004,pp. 162–175.

[17] L. E. Lighfoot, J. Ren, and T. Li, "An energy efficient link-layersecurity protocol for wireless sensor networks", in *Proc. IEEEInt. Con. Elec.-Infor. Technol. EIT 2007*, Chicago, IL, USA, 2007, pp. 233–238.

[18] T. Shon, B. Koo, H. Choi, and Y. Park, "Security architecture for IEEE 802.15.4-based wireless sensor network", in *Proc. 4th Int.Symp. Wirel. Pervasive Comput. ISWPC 2009*, Melbourne, Australia,2009, pp. 1 - 5.

[19] H. Cam, S. Ozdemir, D. Muthuavinashiappan, and P. Nair, "Energy
efficient security protocol for wireless sensor networks", in *Proc.IEEE 58th Veh. Technol. Conf. VTC 2003*, Orlando, Florida, USA,2003, vol. 5, pp. 2981–2984.