Key Encryption in Wireless Sensor Network

Mohammed khalil Ibrahim
Mustansyria University
Computer center

Abstract

The information needed by smart environments is provided by Distributed Wireless Sensor Networks, which are responsible for detecting the relevant quantities, monitoring and collecting the data, assessing and evaluating the information, formulating meaningful user displays, and performing decision-making and alarm functions are enormous. The importance of sensor networks is highlighted by the number of recent funding initiatives, including the DARPA SENSIT program, military programs, and NSF Program Announcements. We described the architecture of sensor networks and present the Important features of security in sensor networks **,** some Types of Attacks on sensor networks and the defense against them finally we propose a public key encryption system by using an algorithm of ElGamal and present the algorithms of encryption , decryption and show the efficiency and security of the proposed system.

1. Sensor Network Architecture

Sensor networks is made up from numbers of nodes with constrains in resources like energy, memory, and computational power and for interaction purposes, the nodes are equipped with radio frequency communication capabilities. However, this wireless communication provides only limited bandwidth. These nodes could be considered as

points of centralized control called base stations. A base station is typically a gateway to another network, a powerful data processing or storage center, or an access point for human interface.

The sensor node has specific factors set also add several constraints for the security architecture. Since only a fraction of the total memory may be used by the cryptographic algorithms and key material, the security architecture demands very lightweight cryptographic algorithms with relatively short key sizes. Furthermore, cryptographic computations need to be executable in an appropriate amount of time as the execution of cryptographic algorithms is not the main task of the nodes. Due to the limited bandwidth and communication being the most expensive operation in terms of energy, messages should not be extended significantly in length when applying security services.

The sensor nodes are equal devices in terms of the role they can play in the network and should self-organize to accomplish their appointed task, without any supervision. Thus, the sensor nodes gather information based on their sensing capabilities and make decisions based upon the gathered data. Another important point in sensor networks is the limited lifetime of sensor data. Sensor data and accordingly events that are derived from it should be communicated in real time.

The network characteristics, similar to the node characteristics, determine important aspects of the desired security architecture. Considering the node mobility, authentication and key exchanges must not depend on numerous extra messages, since the topology is subject to frequent change. Additionally, all necessary cryptographic functions and key material must reside and be executable on the nodes. With respect to the real-time property of sensor networks, cryptographic algorithms should also be as fast as possible. Finally, the security architecture needs to be scalable to accommodate high numbers of nodes.

In a typical WSN we see following network components

- 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 the process itself.
- Gateway or Access points – A Gateway enables communication between Host application and field devices.
- 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.
- Security manager – The Security Manager is responsible for the generation, storage, and management of keys.

2 Important features of security in sensor networks

Setting security features for sensor networks will depend on knowing what it is that needs protecting. Sensor networks share some of the features of mobile ad hoc networks . The four important security features for sensor networks are determined as Confidentiality, Integrity, Authentication and Availability (CIAA).

2.1 Confidentiality

Confidentiality is the ability to blocking messages from a passive attacker so that any message communicated via the sensor network remains confidential.

2.2 Integrity

Data integrity in sensor networks is needed to ensure the reliability of the data and refers to the ability to confirm that a message has not been tampered with, altered or changed while on the network.

2.3 Authentication

Authentication ensures the reliability of the message by identifying its origin. Attacks in sensor networks do not just involve the alteration of packets, adversaries can also inject additional bogus packets. Therefore, the receiving node needs to be able to confirm that a packet received does in fact stem from the node claiming to have sent it. In other words, data authentication verifies the identity of senders.

2.4 Availability

Availability determines whether a node has the ability to use the resources and whether the network is available for the messages to communicate. Since complex security measures entail a higher consumption of energy and computation power, keeping resource starved sensor networks available is challenging. However, failure of the base station or cluster leader's availability will eventually threaten the entire sensor network. Thus availability is of primary importance for maintaining an operational network.

3. Types of Attacks on sensor networks

Sensor networks are particularly vulnerable to several key types of attacks. Attacks can be performed in a variety of ways, most notably as denial of service attacks, but also through traffic analysis, privacy violation, physical attacks, and so on. we will focus first on of some common denial of service attacks and then describe additional attacking, including an identity based attack known as the Sybil attack which is concerned directly with key encryption over networks and between nodes and finally show a review over Attacks Against Privacy.

3.1 Types of Denial of Service attacks

A standard attack on wireless sensor networks is simply to jam a node or set of nodes. Jamming, in this case, is simply the transmission of a radio signal that interferes with the radio frequencies being used by the sensor network. The jamming of a network can come in two forms: constant jamming, and intermittent jamming. Constant jamming involves the complete jamming of the entire network. No messages are able to be sent or received. If the jamming is only intermittent, then nodes are able to exchange messages periodically, but not consistently. This too can have a detrimental impact on the sensor network as the messages being exchanged between nodes may be time sensitive .

Attacks can also be made on the link layer itself. One possibility is that an attacker may simply intentionally violate the communication protocol, IEEE 801.11b (Wi-Fi) protocol, and continually transmit messages in an attempt to

generate collisions. Such collisions would require the retransmission of any packet affected by the collision. Using this technique it would be possible for an attacker to simply deplete a sensor node's power supply by forcing too many retransmissions.

3.2 The Sybil attack

The Sybil attack is defined as a "malicious device illegitimately taking on multiple identities". It was originally described as an attack able to defeat the redundancy mechanisms of distributed data storage systems in peer-to-peer networks . In addition to defeating distributed data storage systems, the Sybil attack is also effective against routing algorithms, data aggregation, voting, fair resource allocation and foiling misbehavior detection. Regardless of the target (voting, routing, aggregation), the Sybil algorithm functions similarly. All of the techniques involve utilizing multiple identities. For instance, in a sensor network voting scheme, the Sybil attack might utilize multiple identities to generate additional "votes." Similarly, to attack the routing protocol, the Sybil attack would rely on a malicious node taking on the identity of multiple nodes, and thus routing multiple paths through a single malicious node.

3.3 Attacks Against Privacy

Sensor network technology promises a vast increase in automatic data collection capabilities through efficient deployment of tiny sensor devices. While these technologies offer great benefits to users, they also exhibit significant potential for abuse. Particularly relevant concerns are privacy problems, since sensor networks provide increased data collection capabilities. Adversaries can use even seemingly innocuous data to derive sensitive information if they know how to correlate multiple sensor inputs. For example, in the famous "panda-hunter problem", the hunter can imply the position of pandas by monitoring the traffic.

The main privacy problem, however, is not that sensor networks enable the collection of information. In fact, much information from sensor networks could probably be collected through direct site surveillance. Rather, sensor networks aggravate the privacy problem because they make large volumes of information easily available through remote access. Hence, adversaries need not be physically present to maintain surveillance. They can gather information in a low-risk, anonymous manner. Remote access also allows a single adversary to monitor multiple sites simultaneously . Some of the more common attacks against sensor privacy are:

- Monitor and Eavesdropping : This is the most obvious attack to privacy. By listening to the data, the adversary could easily discover the communication contents. When the traffic conveys the control information about the sensor network configuration, which contains potentially more detailed information

than accessible through the location server, the eavesdropping can act effectively against the privacy protection.

- Traffic Analysis : Traffic analysis typically combines with monitoring and eavesdropping. An increase in the number of transmitted packets between certain nodes could signal that a specific sensor has registered activity. Through the analysis on the traffic, some sensors with special roles or activities can be effectively identified.
- Camouflage Adversaries can insert their node or compromise the nodes to hide in the sensor network. After that these nodes can masquerade as a normal node to attract the packets, then misroute the packets, e.g. forward the packets to the nodes conducting the privacy analysis.

4 Protection Techniques

We will describe the techniques for satisfying security requirements, and protecting the sensor network from attacks. We start with defending techniques against Denial of Service attacks , Sybil attacks , and Sensor Privacy Attacks .In the end we give a describe for key establishment in wireless sensor networks, which lays the foundation for the security in a wireless sensor network and give a proposal encryption system for secure keys used in wireless sensor network .

4.1 Defending Against Denial of Service attacks

The denial of service attacks are so common , effective defenses must be available to combat them. One strategy in defending against the classic jamming attack is to identify the jammed part of the sensor network and effectively route around the unavailable portion. There are a two phase approach where the nodes along the perimeter of the jammed region report their status to their neighbors who then collaboratively define the jammed region and simply route around it.
To handle jamming at the MAC layer, nodes might utilize a MAC admission control that is rate limiting. This would allow the network to ignore those requests designed to exhaust the power reserves of a node. This, however, is not fool-proof as the network must be able to handle any legitimately large traffic volumes.

Overcoming rogue sensors that intentionally misroute messages can be done at the cost of redundancy. In this case, a sending node can send the message along multiple paths in an effort to increase the likelihood that the message will ultimately arrive at its destination. This has the advantage of effectively dealing with nodes that may not be malicious, but rather may have simply failed as it does not rely on a single node to route its messages.

4.2 Defending Against the Sybil Attack

To defend against the Sybil attack , the network needs some mechanism to validate that a particular identify is the only identity being held by a given physical node .There are two methods to validate identities, direct validation and

indirect validation. In direct validation a trusted node directly tests whether the joining identity is valid. In indirect validation, another trusted node is allowed to vouch for (or against) the validity of a joining node . Newsome et al. primarily describe direct validation techniques, including a radio resource test. In the radio test, a node assigns each of its neighbors a different channel on which to communicate. The node then randomly chooses a channel and listens. If the node detects a transmission on the channel it is assumed that the node transmitting on the channel is a physical node. Similarly, if the node does not detect a transmission on the specified channel, the node assumes that the identity assigned to the channel is not a physical identity.

Another technique to defend against the Sybil attack is to use random key pre-distribution techniques. The idea behind this technique is that with a limited number of keys on a keyring, a node that randomly generates identities will not possess enough keys to take on multiple identities and thus will be unable to exchange messages on the network due to the fact that the invalid identity will be unable to encrypt or decrypt messages.

4.3 Defending Against Attacks on Sensor Privacy

Regarding the attacks on privacy mentioned earlier, there exist effective techniques to counter many of the attacks levied against a sensor. Here we describe several common techniques .

4.3.1 Anonymity Mechanisms Location information that is too precise can enable the identification of a user, or make the continued tracking of movements feasible. This is a threat to privacy. Anonymity mechanisms depersonalize the data before the data is released, which present an alternative to privacy policy-based access control. Researchers have discussed several approaches using anonymity mechanisms, for example, Gruteser and Grunwald analyze the feasibility of anonymizing location information for location-based services in an automotive telematics environment; Beresford and Stajano independently evaluate anonymity techniques for an indoor location system based on the Active Bat.

Total anonymity is a difficult problem given the lack of knowledge concerning a node's location. Therefore, a tradeoff is required between anonymity and the need for public information when solving the privacy problem. Three main approaches are proposed:

- Decentralize Sensitive Data The basic idea of this approach is to distribute the sensed location data through a spanning tree, so that no single node holds a complete view of the original data.
- Secure Communication Channel Using secure communication protocols, such as SPINS , the eavesdropping and active attacks can be prevented.

- Change Data Traffic De-patterning the data transmissions can protect against traffic analysis. For example, inserting some bogus data can intensively change the traffic pattern when needed.
- Node Mobility Making the sensor movable can be effective in defending privacy, especially the location. For example, the Cricket system is a location-support system for in-building, mobile, location dependent applications. It allows applications running on mobile and static nodes to learn their physical location by using listeners that hear and analyze information from beacons spread throughout the building. Thus the location sensors can be placed on the mobile device as opposed to the building infrastructure, and the location information is not disclosed during the position determination process and the data subject can choose the parties to which the information should be transmitted.

5. Key Establishment

One security aspect that receives a great deal of attention in wireless sensor networks is the area of key management. Wireless sensor networks are unique (among other embedded wireless networks) in this aspect due to their size, mobility and computational/power constraints. Indeed, researchers envision wireless sensor networks to be orders of magnitude larger than their traditional embedded counterparts. This, coupled with the operational constraints described previously, makes secure key management an absolute necessity in most wireless sensor network designs. Because encryption and key management/establishment are so important to the defense of a wireless sensor network, with nearly all aspects of wireless sensor network defenses relying on solid encryption, Now we give an overview of the public key encryption and our proposal systems .

6 public key proposal system

Traditionally, key establishment is done using one of many public-key protocols. One of the more common is the Diffie-Hellman public key protocol, but there are many others.

We will propose an encryption system used one of techniques depend on mathematical problems with one direction solutions like discrete logarithm problem with Elgamal algoritham which can summarize as follows:

6.1 ElGamal public-key encryption

The ElGamal public-key encryption scheme can be viewed as Diffie-Hellman key agreement in key transfer mode . Its security is based on the intractability of the discrete logarithm problem and the Diffie-Hellman problem. The basic ElGamal and generalized ElGamal encryption schemes are described in this section.

6.1.1 Definition The *discrete logarithm problem* (DLP) is the following:
given a prime p,a generator α of Z_p*, and an element $\beta \in Z_n^*$, find the integer x , $0 \le x \le p-2$, such that $\alpha^x \equiv \beta (\text{mod } p)$

6.1.2 Definition The *Diffie-Hellman problem (DHP)* is the following: given a prime p:
a generator α of Z_p*, and an element $\alpha^a \bmod p$ *and* $\alpha^b \bmod p$, *find* $\alpha^{ab} \bmod p$.

6.1.3 Basic ElGamal encryption

1. Algorithm Key generation for ElGamal public-key encryption
SUMMARY: each entity creates a public key and a corresponding private key.
Each entity A should do the following:
1. Generate a large random prime p and a generator of the multiplicative group Z_p* of the integers modulo p (using Algorithm 1.1).
2. Select a random integer a, $1 \le a \le p-2$, and compute $\alpha^a \bmod$ p (using Algorithm 1.2).
3. A's public key is (p; α ; α^a)

1.1 Algorithm Selecting a k-bit prime p and a generator α of Z_p*
INPUT: the required bit length k of the prime and a security parameter t.
OUTPUT: a k-bit prime p such that p − 1 has a prime factor ≥ t, and a generator α of Z_p*
1. Repeat the following:
    1.1 Select a random k-bit prime p
    1.2 Factor p − 1.
Until p − 1 has a prime factor ≥ t.
2. Use Algorithm 1.1.1 with G = Z_p* and n = p − 1 to find a generator α of Z_p*
3. Return(p, α).

1.1.1 Algorithm Finding a generator of a cyclic group
INPUT: a cyclic group G of order n, and the prime factorization $n = p_1^{e1} p_2^{e2} \ldots p_k^{ek}$
OUTPUT: a generator α of G.
1. Choose a random element α in G.
2. For i from 1 to k do the following:
    2.1 Compute $b \leftarrow \alpha^{n/pi}$
    2.2 If b =1then go to step 1.
3. Return(α).

1.2 Algorithm Repeated square-and-multiply algorithm for exponentiation in Z
INPUT: a ∈ Z_n , and integer 0≤ k < n whose binary representation is $k = \sum_{i=0}^{t} k_i 2^i$
OUTPUT: a^k mod n.
1. Set b←1.If k =0 then return (b).
2. Set A← a.
3. If k_0=1 then set b ← a.

4. For i from 1 to t do the following:
   4.1 Set A←A^2 mod n.
   4.2 If k_i = 1then set b←A . b mod n.
5. Return(b).

2. Algorithm ElGamal public-key encryption

SUMMARY: B encrypts a message m for A, which A decrypts.

1. *Encryption.* B should do the following:

(a) Obtain A's authentic public key (p; α ; α^a).

(b) Represent the message as an integer m in the range {0, 1, …,p− 1}.

(c) Select a random integer k, $1 \le k \le p-2$

(d) Compute $= \gamma = \alpha^k \bmod p$ *and* $\delta = m \,.\, (\alpha^a)^k \bmod p$.

(e) Send the cipher text c = (γ, δ) to A.

2. *Decryption.* To recover plaintext m from c, A should do the following:

(a) Use the private key a to compute γ^{p-1-a} mod p (note $\gamma^{p-1-a} = \gamma^{-a} = \alpha^{-ak}$)

(b) Recover m by computing $((\gamma^{-a}) \cdot \delta \bmod p$

6.2 efficiency of ElGamal encryption

(a) The encryption process requires two modular exponentiations, namely α^k mod p and $(\alpha^a)^k$ mod p. These exponentiations can be sped up by selecting random exponents k having some additional structure.

(b) ElGamal encryption is one of many encryption schemes which utilizes randomization in the encryption process. The fundamental idea behind randomized encryption techniques is to use randomization to increase the cryptographic security of an encryption process through one or more of the following methods:

(i) increasing the effective size of the plaintext message space;

(ii) precluding or decreasing the effectiveness of chosen-plaintext attacks by virtue of a

one-to-many mapping of plaintext to ciphertext .

(iii) precluding or decreasing the effectiveness of statistical attacks by leveling the a priori

probability distribution of inputs.

(c) A disadvantage of ElGamal encryption is that there is *message expansion* by a factor of 2. That is, the ciphertext is twice as long as the corresponding plaintext.

6.3 security of ElGamal encryption

(a) The problem of breaking the ElGamal encryption scheme, i.e., recovering m given

$p, \alpha, \alpha^a, \gamma$ *and* δ is equivalent to solving the Diffie-Hellman problem . In fact, the ElGamal encryption scheme can be viewed as simply comprising a DiffieHellman key exchange to determine a session key α^{ak} and then encrypting

the message by multiplication with that session key. For this reason, the security of the ElGamal encryption scheme is said to be *based* on the discrete logarithm problem in Z_p*, although such an equivalence has not been proven.

(b) It is critical that different random integers k be used to encrypt different messages.

Suppose the same k is used to encrypt two messages m_1 and m_2 and the resulting ciphertext pairs are (γ_1, δ_1) and (γ_2, δ_2). Then $\delta_1 / \delta_2 = m_1 / m_2$ and m_2 could be easily computed if m_1 were known.

6.4 Generalized ElGamal encryption

The ElGamal encryption scheme is typically described in the setting of the multiplicative group Z_p*, but can be easily generalized to work in any finite cyclic group G. As with ElGamal encryption, the security of the generalized ElGamal encryption scheme is *based* on the intractability of the discrete logarithm problem in the group G. The group G should be carefully chosen to satisfy the following two conditions:

1. for *efficiency*, the group operation in G should be relatively easy to apply; and
2. for *security*, the discrete logarithm problem in G should be computationally infeasible. The following is a list of groups that appear to meet these two criteria:

1. The multiplicative group Z_p* of the integers modulo a prime p.
2. The multiplicative group F_{2m}^* of the finite field F_{2m} of characteristic two.
3. The group of points on an elliptic curve over a finite field.

7. Conclusion

After studying the wireless sensor networks Architecture and all security issue and present some attacks on this networks and numbers of solutions. we propose a key encryption systems based on the intractability of the discrete logarithm problem and the Diffie-Hellman problem (i.e) The encryption process requires two modular exponentiations, namely $\alpha^k \bmod p$ and $(\alpha^a)^k \bmod p$. These exponentiations can be sped up by selecting random exponents k having some additional structure like increasing the effective size of the plaintext message space and decreasing effectiveness of chosen-plaintext attacks and decreasing effectiveness of statistical attacks which can increase the security of data transferred within these networks.

The ElGamal encryption scheme which used in our proposed system is typically described in the setting of the multiplicative group Z_p* which must be chosen to satisfy the following two conditions:

1. for efficiency, the group operation in Z_p^* should be relatively easy to apply; and
2. for security, the discrete logarithm problem in Z_p^* should be computationally infeasible.

Our proposed system which based on ElGamal encryption scheme have some disadvantage because of the message is expansion by a factor of 2. That is, the ciphertext is twice as long as the corresponding plaintext. And the second disadvantage is by using different random integers k to encrypt different messages if two messages m1 and m2 encrypted with same key then if computed m1 the m2 is also will be computed

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. IEEE Communications Magazine, 40(8):102–114, August 2002.

[2] A. R. Beresford and F. Stajano. Location Privacy in Pervasive Computing. IEEE Pervasive Computing, 2(1):46–55, 2003.

[3] D. W. Carman, P. S. Krus, and B. J. Matt. Constraints and approaches for distributed sensor network security. Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood, MD, 2000.

[4] H. Chan and A. Perrig. Security and privacy in sensor networks. IEEE Computer Magazine, pages 103–105, 2003 2003.

[5] J. Douceur. The sybil attack. In Proc. of the 1st International Workshop on Peer-to-Peer Systems (IPTPS'02), February 2002.

[6] M. Gruteser and D. Grunwald. A methodological assessment of location privacy risks in wireless hotspot networks. In First International Conference on Security in Pervasive Computing, 2003. [28] M. Gruteser, G. Schelle, A. Jain, R. Han, and D. Grunwald. Privacy-aware location sensor networks. In 9th USENIX Workshop on Hot Topics in Operating Systems (HotOS IX), 2003.

[7] N. Gura, A. Patel, A. Wander, H. Eberle, and S. Shantz. Comparing elliptic curve cryptography and rsa on 8-bit cpus. In In 2004 workshop on Cryptographic Hardware and Embedded Systems, August 2004.

[8] D. J. Malan, M. Welsh, and M. D. Smith. A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography. In First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON, 2004.

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

[10] C. Ozturk, Y. Zhang, and W. Trappe. Source-location privacy in energyconstrained sensor network routing. In Proceedings of the 2nd ACM workshop

on Security of Ad hoc and Sensor Networks, 2004.
[11] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler. Spins: security
protocols for sensor networks. Wireless Networking, 8(5):521–534, 2002.
[12] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan. The cricket locationsupport system. In Proc. of the Sixth Annual ACM International Conference on Mobile Computing and Networking (MOBICOM), August 2000.
[13] B. Schneier. Applied Cryptography. Second Edition, John Wiley & Sons, 1996.
[14] A. Smailagic, D. P. Siewiorek, J. Anhalt, and Y. Wang D. Kogan. Location sensing and privacy in a context aware computing environment. In Pervasive
Computing, 2001.
[15] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus. Tinypk: securing sensor networks with public key technology. In Proceedings of the 2nd ACM workshop on Security of Ad hoc and Sensor Networks (SASN '04), pages 59–64, New York, NY, USA, 2004. ACM Press.
[16] A. D. Wood and J. A. Stankovic. Denial of service in sensor networks. Computer, 35(10):54–62, 2002.
[17] http://www.zigbee.org/, 2005.
[18] L.M. A DLEMAN, "A subexponential algorithm for the discrete logarithm problem with applications to cryptography", *Proceedings of the IEEE 20th Annual Symposium on Foundations of Computer Science*, 1979.
[19] L.M. ADLEMAN AND J. DEMARRAIS,"A subexponential algorithm for discrete logarithms over all finite fields", *Mathematics of Computation*, (1993).
[20] L. M. A DLEMAN,J.DEMARRAIS, AND M.D. H UANG, "A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields", *Algorithmic Number Theory (LNCS 877)*, 1994.
[21] ANSI X9. 42, "Public key cryptography for the financial services industry: Management of symmetric algorithm keys using DiffieHellman", draft, 1995.