Wireless Sensor Network, 2012, 4, 155-161
http://dx.doi.org/10.4236/wsn.2012.46022 Published Online June 2012 (http://www.SciRP.org/journal/wsn)

An Efficient Key Management Scheme for Hierarchical Wireless Sensor Networks

Benamar Kadri[1], Djilalli Moussaoui[1], Mohammed Feham[1], Abdellah Mhammed[2]
[1]STIC Lab., Department of Telecommunications, University of Tlemcen, Tlemcen, Algeria
[2]Telecom SudParis, Evry, France
Email: benamarkadri@yahoo.fr

Received December 29, 2011; revised March 10, 2012; accepted April 19, 2012

ABSTRACT

The recent advances in integrated circuit technologies, microprocessor hardware, wireless communications, embedded systems and technologies as well as the emergence of Ad-hoc networking, made up the concept of wireless sensor networks. Regarding the nature of sensors and the nature of the environment of deployment sensor networks are exposed to many attacks more than any other networks, therefore new strategies and protocols of security must be defined for these networks taking into consideration the characteristics of sensors as well as the architecture of the network. In this paper we propose a lightweight implementation of public key infrastructure called cluster based public infrastructure (CBPKI), CBPKI is based on the security and the authenticity of the base station for executing a set of handshakes intended to establish session keys between the base station and sensors over the network used for ensuring data confidentiality and integrity.

Keywords: WSN; Security; PKI; CBPKI; Clustering; Key Management

1. Introduction

Last years have known the development of small, low cost, low power and multifunctional sensor nodes, having the possibility of sensing and collecting application specific data as temperature, pressure and movement to allow environment monitoring [1]. These sensors networked with short range wireless medium are called wireless sensor networks WSN, which is a collection of hundreds to thousands of sensor nodes wirelessly connected to each other and used as an infrastructure for forwarding the environment measures to a sink node or a base station. Sensors are deployed in a large area without any centralized or administrative authority or infrastructure, collaborating for maintaining connectivity with the base station using multi hop links [2].

The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian applications, including environment and habitat monitoring, healthcare applications, home automation, traffic control, and environmental monitoring [3].

Regarding their nature as well as their field of application sensor networks seem to be part of unpredictable and hostile environment where the aspect of security must be carefully carried out, to guaranty the services of security such as confidentiality, integrity and authentication and resist against the increasing number of attacks, all these aspects must be considered under the constrained nature of sensors, usually limited in energy and computing power. In literature several strategies were proposed to secure WSN, however the majority of them are based on symmetric cryptography which could not guaranty efficiently the security services and resist against attacks.

In this paper we are going to present a simplified public key infrastructure based on the authenticity of the base station as a secure entity, responsible of security establishment over the network.

The proposed scheme is called cluster based public key infrastructure CBPKI is intended to be executed over hierarchical networks, in which the base station and cluster heads play the key role for securing data transmission, by collaborating for executing handshakes and key updates.

2. Sensor Network Architectures

Generally, a wireless sensor network is composed of a set of sensors randomly deployed in a large region without any infrastructure or centralized authority. Therefore, sensors must collaborate between themselves to achieve the network goals as well as the network usual services for maintaining a secured and efficient connectivity with the base station. Mainly, two architectures for sensor networks [4] exist.

2.1. Flat Network Architecture

The flat architecture is the simplest way to deploy a wireless sensor network, in the way that sensors are randomly deployed in a defined area without taking into consideration the characteristics of sensors neither the environment of deployment. Sensors are responsible of establishing and securing the connection with the base station. In such architecture, sensors are equal in capacities and any negotiation with the base station is done individually by each sensor.

Flat architecture is suitable for stable networks where the collected reports are not numerous, since the routing overhead of a flat network is very important due to flooding used for route discovery.

2.2. Hierarchical Network Architecture

Due to the complexity of managing a flat network caused by the increasing number of sensors as well as the number of reports sent to the base station, the hierarchical architecture tries to simplify the management of the network by organizing sensors into groups called clusters. One of the members of the cluster is elected as cluster head responsible of additional tasks such as cluster management, the rest of sensors are called cluster members.

The hierarchical architecture simplifies considerably the network management, by delegating some redundant tasks to the cluster head which minimize considerably the overhead due to the execution of these tasks by each sensor individually. In addition a hierarchical architecture can be efficiently used for data aggregation, in which the cluster head play the role of the aggregator.

Hierarchical architecture for managing security or routing seems to be more promising since the cluster head is intended to play the key role for security or routing which minimizes the number of operations for executing the elementary operations for routing or security protocol since a subset of operations is delegated to the cluster head.

3. Security in Wireless Sensor Network

3.1. Attacks against WSN

Due to the nature of implied devices in sensor networks, generally small electronic devices with limited resources and capacities as well the used medium which is the radio waves naturally opened to anyone with the adequate hardware and software, making wireless sensor networks exposed to several attacks more than any other networks, ranging from passive, active and physical attacks:

Capture attack**:** this is a physical attack, in which an attacker gain access to sensors' hardware, in order to perturb the functioning of the network by damaging the captured sensors or to get the stored cryptographic keys to execute other kind of attacks against the network protocols, this attack is out of scope of this paper since it cannot be detected using a security scheme [5].

Eavesdropping**:** this passive attack is the simplest attack against an opened network, in which an attacker with the adequate hardware and software passively listen the exchanged data over the network in order to get information about the structure of the network and the underlying routing protocols which can be used for future active attacks [5].

Sinkhole**:** also called black hole, its objective is to attract the traffic from a particular area through a compromised node, by injecting false routing information advertising the attacker as the legitimate sink node or having the shortest path to the base station which redirects the network traffic over the attacker [6], in order to stop the network service or to execute other attacks such as man in the middle, data modification or eavesdropping, replay, etc.

Spoofing attacks**:** also called impersonate attack is executed in the absence of an authentication mechanism, in the way that the attacker spoofs the identity of a legitimate node in order to gain access to the network or to execute malicious actions using the spoofed identity, this attack presents a great risk if the spoofed identity is the base station which means that all the sensed data is sent to the false base station [6].

Denial of service attacks**:** this kind of attacks are the most dangerous attacks against wireless networks, where the attacker tries to disrupt, deny, degrade the service of the network, it is planned in different manner and decreases network lifetime in different ways. Among all the denial of service attacks the flooding attack is executed against wireless sensor networks, in which an attacker broadcast permanently hello messages which are rebroadcasted by each sensor over the network, which consumes the network bandwidth, sensor nodes resources and decreases the network lifetime [7].

Selective forwarding**:** in selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any more. In contrary of black hole attack which can be easily detected, in selective forwarding the adversary selectively forwards packets and drop or modifies packets originating from a defined area or nodes and forwards the remaining traffic which can complicate its detection [8].

3.2. Previous Works

In literature the aspect of security in WSN was treated with a great consideration to the limited resources of sensors such as computing, energy and storage capacities. This has given birth to a variety of scheme based essentially on symmetric cryptography which makes them vulnerable against several attacks. In this section we give an overview of the most known security schemes:

Shared key**:** this solution is the simplest way for securing WSN; it uses a single shared key to encrypt traffic over the network. In this scheme an off-line dealer preload the key in sensors before deployment, then each sensor uses this key to decrypt traffic and join the network. As any other scheme based on single shared key, this scheme is vulnerable against capture attack which is more possible in sensor network, since the capture of only one sensor can compromise the shared key and then the whole network [9].

Secure pebblenets**:** this solution proposed by Basagni [10] is an extended version of the shared key solution. By using a set of symmetric keys preloaded to each sensor over the network, which is divided into cluster in order to simplify the management of security. Intra cluster communication is managed individually by the cluster-head using a predefined symmetric key which guaranties the continuation of data aggregation, inter cluster communication, data confidentiality and integrity are managed using another set of keys.

Tinysec**:** is a link layer security protocol based on symmetric key encryption, TinySec [11] supports two different security options: authenticated encryption (TinySec-AE) and authentication only (TinySec-Auth). This scheme can be used over a tinyOS. The use of MAC layer security instead of end to end security may avoid denial of service attacks. However, this protocol does not define any strategy to deliver and distribute cryptographic keys; otherwise this protocol can be used by any other key management scheme as an underlying tool for encryption.

Simplified SSL handshake**:** in [12], the authors give the energy cost analysis of a simplified version of SSL applied to WSN, which reduces the amount of exchanged data between any pair of nodes to save energy and bandwidth. The simplified handshake is used to setup a secure key between sensors or sensors and the base station in the network as the original SSL. Compared to the original SSL protocol this proposition is more energy saving however it is not energy efficient, since a handshake between each pair of sensors consumes lot of sensor resources.

4. Public Key Infrastructure for WSN

Public key infrastructure is recognized as the most efficient and powerful tool for managing security in conventional network, since it guaranties all the security service such as integrity, confidentiality and authentication. PKI is essentially based on a third party called Certificate Authority (CA) responsible of creating and managing the distribution, revocation and the renewal of digital certificate, depending on the application or the nature of the network other component such as Registration Authority (RA) and Certificate Revocation List (CRL) are deployed in a PKI [6].

PKI has been efficiently deployed for conventional networks, since the existence of a secured CA is possible, however for a wireless ad hoc network, it is not guaranteed that a complete implementation of a PKI is possible, due to the absence of infrastructure as well as the risks to which is exposed any certificate authority such as physical attack. Therefore, the security schemes developed for wireless sensor networks are generally based on symmetric key encryption which is more efficient regarding the resource consumption such as energy, CPU and memory which are very crucial in wireless networks, however some schemes such as shared key and Tinysec [11] are not complete and still vulnerable against lot of attacks since they don't guaranty the authenticity of the communicating entities as well as the integrity of the transmitted data.

Although, a complete solution to guaranty the security services must be based on public key cryptography in order to guaranty the authentication of wireless nodes over the network using a pair of keys, one of the keys is used for encryption called private key and the second one is publicly known within the network used for decrypting messages encrypted with the private key, which guaranties data authentication, integrity and confidentiality. Nevertheless, Public key cryptography is omitted from the use in WSN, due to its great consumption of energy and bandwidth which are very crucial in sensor networks. However, last years have known the development of new cryptographic algorithms more energy efficient and giving the same threshold of security as the conventional algorithms such as RSA [13]. Elliptic Curve Cryptography (ECC) [14] is one of these new algorithms and it is the most promising regarding the energy and time consumption, which makes it very suitable for data encryption in WSN.

5. Cluster Based PKI

As described above, a wireless sensor network suffers from great problems of security due to the nature of sensors as well as the nature of environment of deployment. In the other hands the majority of security schemes proposed in literature are based on symmetric encryption making them vulnerable against several attacks, since a robust security scheme must guaranty all the security services including integrity, confidentiality and authentication which can only be achieved by using a combination of several encryption techniques.

In this section we are going to present a hierarchical security scheme called CBPKI based on a set of handshakes intended to establish secure tunnels between each communicating entities over the networks.

Using these handshakes the base station shares with each sensor over the network a symmetric cryptographic key used for encrypting ordinary traffic over the network for data confidentiality, we also propose to use message authentication code MAC for ensuring integrity as well as public key cryptography to ensure authenticity over the networks

5.1. Assumption on Sensors

In order to make in practice our scheme, we suppose that before the network deployment each sensor receives the public key of the base station from an off-line dealer in order to guaranty the authentication of the base station by the network sensors. Since the base station is the unique entity having a pair of asymmetric keys.

We suppose also that the hierarchical architecture is already established, in other words the network is divided into clusters where one of the members of each cluster is elected to be cluster head using one of the clustering algorithms proposed in literature. The cluster head is supposed to be the most powerful sensor in its cluster regarding the battery and CPU power, since this node has more tasks to be done compared to the rest of its cluster members such as data aggregation and handshake execution.

For the system functioning we assume that:

- The base station have more computational and energy power compared to sensors.
- The base station has a pair of keys (private and public key).
- Each sensor is capable to use:
  - Asymmetric Cryptography: To provide authentication of the base station.
  - Symmetric Cryptography: To ensure the confidentiality of traffic across the network.
  - MAC (message authentication code) to ensure data integrity.
- Each sensor has the capacity to save at least the public key of the base station and a session key used for data encryption.
- Each sensor receives the public key of the base station by an off-line dealer.

5.2. CBPKI Handshakes

As described above CBPKI is intended to establish security over the network using three cryptographic methods destined to establish all the security services. To achieve this, CBPKI is based on two handshakes:

Cluster-head to base station handshake**:** this handshake is intended to share a symmetric key used for securing end to end communication between each cluster head and the base station.

Cluster members handshake**:** this handshake is executed by sensors and it is intended to distribute the session key shared by the base station and each cluster member within a given cluster.

5.3. Cluster-Head to Base Station Handshake

The handshake is executed by each cluster head and the base station is intended to establish a symmetric key between sensors and the base station. This handshake is executed in three steps:

Hand shake launching**:** the cluster head to base station handshake is launched by each cluster head over the network, by generating a random symmetric key, the cluster head encrypts this key with the public key of the base station and sends it to the base station using the underlying routing protocol in an ordinary packet.

The use of the public key for transporting the session key ensures the authentication of the base station, as well as the integrity and the confidentiality of the handshake.

Establishment of the session key**:** after receiving and decrypting the message containing the session key coming from each cluster head using the corresponding private key since only the base station has the valid private key which guaranty the authentication, the integrity and the confidentiality of the handshake, the base station stores the symmetric key with the identifier of the cluster head in a global table used for identifying and managing clusters over the network.

Completion of the handshake**:** in order to validate the handshake the base station encrypts a challenge message for each cluster head using the established session key. Each cluster head decrypts the message sent by the base station if the operation success the handshake is successfully completed otherwise an attack is supposed; and a new handshake is launched until a valid session key is established (**Figure 1**).

5.4. Cluster Members Handshake

After a successful cluster head to base station handshake, each cluster head shares with the base station a symmetric encrypting key, therefore each cluster member must get the same session key; in order to be used for data aggregation between the cluster head and its cluster members. The distribution of the session key is done by the base

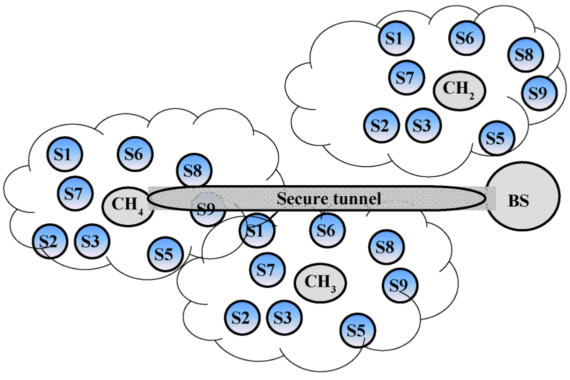

Figure 1. Secure tunnel over hierarchical network.

station since the base station is the unique authenticated entity over the network.

So, each cluster member builds a message containing the identifier of its cluster head and a symmetric key used to secure this operation, this message is encrypted by the public key of the base station.

When the base station receives this message, it seeks the existence of the corresponding session key of the cluster head (established during the previous handshake), encrypts it with the session key sent by the sensor and sends it to the corresponding cluster member.

The dialogue is done with the base station instead of the cluster head because the base station is authenticated using the public key distributed before deployment.

Each sensor when receives this message from the base station, shares the same session key with its cluster head and the base station.

5.5. System Functioning

After the achievement of the previous handshakes, each sensor over the network shares a symmetric key with its cluster head and the base station which guaranties:

- The confidentiality of the exchanged data between the base station, cluster head and cluster members.
- All the handshakes and traffic exchanging are authenticated using the public key of the base station.
- The operations of data aggregation are always possible.
- A proactive key update is possible to guaranty more robustness.

In order to ensure the last security service which is data integrity, we propose to use a message authentication code MAC encrypted with the session key. Therefore, each packet is passed in a hash function to obtain a finger print which is encrypted by the session key shared with the base station.

The structure of the packet stays unchanged only a field containing the encrypted finger print is added at the end of the packet which could not affect the global structure of the network stack.

Another option can be used for more security depending on the importance and the nature of the networks is to encryption the MAC joined to each packet by the public key of the base station, this option consumes more energy due to the additional overhead for encryption however it guaranties the maximum of security (**Figure 2**).

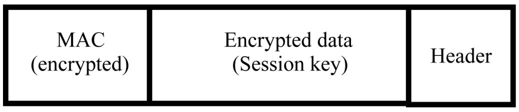

Figure 2. Packet structure.

5.6. Key Update

A wireless sensor networks is deployed for a long period; which makes it subject of long term attacks in which the attacker tries to get the encrypting key by cumulating a great amount of encrypted data and uses some vulnerabilities of the encrypting algorithms, or simply uses this data to launch reply or routing attacks.

Therefore we propose to launch periodically a proactive key update of the session key; the period of the key update is defined by the administrator according to the length of the used keys as well as the robustness of the encrypting algorithms.

The key update is launched by the cluster head using the same hand shake defined above in order to establish a new session key between the base station and the cluster head. After updating the session key of the cluster head, each cluster head encrypts a copy with the old session key for each member of its cluster. The new session key will be automatically used after receiving the message by sensors in a given cluster.

5.7. Joining the Network

A wireless sensor network is supposed to increases in size, so permanently new sensors join the network. In order to join this sensor into the network security, we suppose that the administrator of the network load the public key of the base station into the new sensors. Using this key it can launch a handshake with the base station and join one of the nearest clusters.

6. Analysis

6.1. Energy Cost

CBPKI uses two types of cryptography, symmetric and asymmetric algorithms with an optional use of a hash function as a MAC (message authentication code). We propose to use the ECC (Elliptic Curve Cryptography) for data encryption considered to be more efficient regarding energy consumption.

Taking into consideration the size of session keys (check sum, ID), the maximum packet size will not exceed the 512-bit so the consumed energy for its transmission is 3.78 mJ and 1.83 mJ for reception, using as platform Mica2dots [15], the energy consumed for data encryption and decryption is 22.82 mJ for asymmetric encryption and 0.039 mJ for symmetric encryption. Therefore the total energy consumption for each handshake is 28.47 mJ (**Table 1**).

6.2. Security Services

The robustness of a key management scheme is defined according to its capability to guaranty the basic security services which are:

***Confidentiality*:** data confidentiality is defined as the guaranty that the transmitted data is not understood by

Table 1. Energy cost of base station to sensor handshake.

Operations		Energy (mJ)
Base station to Sensor handshake	Encrypt session key	22.82
	Send session key	3.78
	Receive session key	1.83
	Decrypt challenge message	0.039
Total energy cost		28.47
Key update for cluster members		0.039
Key update for cluster heads		28.47

anyone but the legitimate communicating nodes. The proposed scheme uses symmetric encryption to ensure this aspect. We have also proposed to enforce security by a periodic key update to prevent long term attacks.

Authentication: this aspect deals with the authenticity of the communicating parties over the network, in order to prevent impersonate attacks. To treat this aspect we have used public key encryption in order to authenticate the base station as well as sensors over the network, since only legitimate sensors have the valid public key of the base station which is pre-installed in each deployed sensor.

Integrity: the integrity of data deals with the possibility of detect data modification of the transmitted data, to guaranty this criterion we have used a MAC (Message authentication codes) computed and joined to each sent packet between the base station and any sensor over the network, this MAC is encrypted with the public key of the base station or the established session keys between the base station and sensors which guaranty a full authenticity and integrity of data.

6.3. Resistance to Attacks

In this paragraph, we try to evaluate the robustness of our solution regarding security threats. By the way, we will focus on different main attacks:

Eavesdropping: this attack is avoided in our approach using symmetric key encryption with proactive key update to enforce security.

Spoofing attacks: using our approach it seems that this attack can’t be executed since the base station is authenticated using a public key preloaded on sensors before deployment which ensure a mutual authentication between the base station and sensors over the network.

Data modification and insertion: these kinds of attacks alter the integrity of the exchanged data, as devoted above all these attacks are easily avoided by the encryption as method for data integrity. So only authenticated nodes can insert or modify data over the network.

Flooding attacks: this attack consists to saturate the energy of sensors by rebroadcasting false hello messages. This attack has not a great effect on our proposed scheme since only message originated from authenticated sensors are rebroadcasted and the rest of messages are rejected.

Sinkhole attack: this attack tries to attract the traffic over a malicious node in order to control, reply or modify messages coming from a certain region or sensors; this attack is based on falsifying message sent to the base station which is impossible because message sent to the base station are encrypted.

Avoiding other attacks: the proposed scheme is based on a set of handshakes to establish encrypting keys used by the bases station and the rest of sensors in order to secure end to end communication, which avoids the majority of attacks based on traffic analysis, the proposed scheme can also be used as a tool for key distribution in order to deliver encrypting keys for routing protocol which enforce the security of the network and detect any other attack using intrusion detection systems.

7. Conclusion

In this paper we have presented a security scheme based on public key cryptography, cluster based public key infrastructure is a simplified version of conventional public key infrastructure, in the way that it uses the public key of the base station in order to ensure the authentication of the base station considered to be the secured authority in a WSN. CBPKI uses a set of handshakes intended to establish symmetric encrypting keys between network sensors and the base station, these session keys are used to ensure data confidentiality over the network and data integrity by using message authenticated code. Regarding the security services, it seems that CBPKI ensure all security services and it is robust against several attacks with low power consumption and network overhead.

REFERENCES

[1] J. Zheng and A. Jamalipour, “Wireless Sensor Networks: A Networking Perspective,” John Wiley & Sons, Hoboken, 2009.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, “Wireless Sensor Networks: A Survey,” C*omputer Networks*, Vol. 38, No. 4, 2002, pp. 393-422. doi:10.1016/S1389-1286(01)00302-4

[3] C. F. Garcia-Hermandez, *et al.*, “Wireless Sensor Networks and Applications,” *International Journal of Computer Science and Network Security*, Vol. 7, No. 3, 2007, pp. 264-273.

[4] D. Karaboga, S. Okdem and C. Ozturk, “Cluster Based Wireless Sensor Network Routings Using Artificial Bee Colony Algorithm,” *International Conference on Autonomous and Intelligent Systems* (*AIS*), Povoa de Varzim, 21-23 June 2010, pp. 1-5. doi:10.1109/AIS.2010.5547042

[5] G. Padmavathi and D. Shanmugapriya, “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks,” *International Journal of Computer Sci-*

ence and Information Security, Vol. 4, No. 1-2, 2009.

[6] T. Kavitha and D. Sridharan, "Security Vulnerabilities in Wireless Sensor Networks: A Survey," *Journal of Information Assurance and Security*, Vol. 5, No. 1, 2010, pp. 31-44.

[7] A. D. Wood and J. A. Stankvic, "Denial of Service in Sensor Networks," *IEEE Computer*, Vol. 35, No. 10, 2002, pp. 54-62. doi:10.1109/MC.2002.1039518

[8] S. De, C. Qiao and H. Wu, "Meshed Multipath Routing with Selective Forwarding: An Efficient Strategy in Wireless Sensor Networks," *Computer Networks*, Vol. 43, No. 4, 2003, pp. 481-497. doi:10.1016/S1389-1286(03)00355-4

[9] S. Rafaeli and D. Hutchison, "A Survey of Key Management for Secure Group Communication," *ACM Computing Survey*, Vol. 35, No. 3, 2003, pp. 309-329. doi:10.1145/937503.937506

[10] S. Basagni, K. Herrin, *et al.*, "Secure Pebblenets," *Proceedings of the* 2nd *ACM International Symposium on Mobile ad hoc Networking & Computing*, Long Beach, 4-5 October 2001, pp. 156-163.

[11] C. Karlof, N. Sastry and D. Wagner, "Tinysec a Link Layer Security Architecture for Wireless Sensor Net-Works," *Second ACM Conference on Embedded Net-Worked Sensor Systems*, Baltimore, 3-5 November 2004, pp. 162-175.

[12] A. S. Wander, N. Gura, H. Eberle, V. Gupta and S. C. Shantz, "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks," *Proceedings of* 3rd *IEEE International Conference on Pervasive Computing and Communications*, Kauai Island, 8-12 March 2005, pp. 324-328.

[13] A. S. Wander, N. Gura, H. Eberle, V. Gupta and S. C. Shantz, "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks," *Proceedings of* 3rd *IEEE International Conference on Pervasive Computing and Communications*, Kauai Island, 8-12 March 2005, pp. 324-328.

[14] N. Gura, A. Patel, A. Wander, H. Eberle and S. C. Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-Bit CPUs," *Proceedings of the Sixth Workshop on Cryptographic Hardware and Embedded Systems*, Cambridge 11-13 August 2004, pp. 119-132. doi:10.1007/978-3-540-28632-5_9

[15] Crossbow Technology Inc., Processor/Radio Modules, 2008. http://www.xbow.com