IJIRR

International Journal of Information Research and Review
Vol. 03, Issue, 11, pp. 3168-3172, November, 2016

Research Article

THE IMPORTANCE OF THE CRYPTOGRAPHY BASED ON ELLIPTIC CURVES IN WIRELESS SENSOR NETWORKS SECURITY

[1,*]Mohammed Said SALAH, [1,2]Abderrahim Maizate and [1]Mohammed OUZZIF

[1]RITM-ESTC / CED-ENSEM, University Hassan II, Km 7, Eljadida Street, B.P. 8012 Oasis, Casablanca, Morocco
[2]STIC Laboratory, Chouaib Doukkali University, El Jadida, Morocco

ARTICLE INFO

Article History:

Received 28th August, 2016
Received in revised form
22nd September, 2016
Accepted 24th October, 2016
Published online November, 30th 2016

Keywords:

WSN,
Security,
ECC,
RECC-D,
RECC-C,
CECKM,
AVL…

ABSTRACT

Wireless sensor networks are ubiquitous in monitoring applications, medical control, environmental control and military activities… In fact, a wireless sensor network consists of a set of communicating nodes distributed over an area in order to measure a given magnitude, or receive and transmit data independently to a base station which is connected to the user via the Internet or a satellite, for example. Each node in a sensor network is an electronic device which has calculation capacity, storage, communication and power. However, attacks in wireless sensor networks can have negative impacts on critical network applications leading to the minimization of security within these networks. So it is important to secure these networks in order to maintain their effectiveness. In this paper, we have initially attempted to study approaches oriented towards cryptography and based on elliptic curves, then we have compared the performance of each method relative to others.

INTRODUCTION

Thanks to wireless sensor networks, we can now monitor and control physical parameters (Bachir and Dohler, 2010). WSNs have applications in many areas (Karl and Willig, 2005), including the observation of nature and the environment, security of buildings and home automation, traffic management, medical monitoring, or military operations. In many applications of sensor networks, data can be threatened by external events that should not occur during normal network operations (Dietrich and Dressler, 2009). The reliability and security of data carried in a WSN depends on several parameters including energy resources (Boyle, 2007), types of protocols used for routing, and transport of data. Ensuring such characteristics is not an easy task to achieve, especially when the nodes are composed of electronic devices with limited hardware capabilities.

Corresponding author: Mohammed Said SALAH,
[1]RITM-ESTC / CED-ENSEM, University Hassan II, Km 7, Eljadida Street, B.P. 8012 Oasis, Casablanca, Morocco.

Multiple security approaches we will see in detail have the objective of secure communication between nodes in a wireless sensor network. Each approach has advantages, limitations and may be used according to a specific need. The remaining parts of this paper will focus on the following: In Section II, we introduce wireless sensors and modules of a sensor (Roth *et al*., 2010), and the role of each component. Then, we shall present the characteristics of a wireless sensor networks WSN, the security constraints in WSN (Munivel, 2010), and vulnerabilities in a network of sensors.

By the end of the section, we will offer an analysis of vulnerable attackers and attacks. In Section III, we shall present the different approaches of cryptography based on elliptic curves. In the last section, we analyze the different approaches and compare the performance of each method by looking at: the memory used by nodes for storing ECC keys (http://www.dice.ucl.ac.be/crypto/.GC-19951l, pages), the average energy consumed per node and the number of packets exchanged when installing keys.

Wireless Sensor Networks

Characteristics of Wireless Sensor Network WSN

A wireless sensor network has the following characteristics (Karl and Willig, 2005):

- Lack of infrastructure - sensor networks in particular differ from other networks through the absence of pre-existing infrastructure.
- Important size - a network sensor may contain thousands of nodes.
- Interference - the radio links aren't isolated, two simultaneous transmissions on the same frequency, or on similar frequencies can interfere.

Dynamic Topology - the sensors can be attached to mobile objects moving freely and arbitrarily (Kuntz *et al*., 2011).

- Limited physical security - Wireless sensor networks are more affected by security settings than by traditional wired networks.

Constraint of energy (Landsiedel *et al*., 2012)- the most critical feature in sensor networks is the modesty of its energy resources because each network sensor has few resources in terms of energy (battery).

The vulnerabilities of wireless sensor networks

Vulnerabilities are weaknesses of a system that the attacker exploits to gain privileges. (Gura *et al*., 2004) There are two types of vulnerabilities in a sensor network WSN:

- Physical vulnerability is a means of attack, which allows the attacker to change in part a sensor, for example by changing its programming code, or by copying protection keys for reuse in a new attack.

The vulnerability lies in logic programs and protocols. It appears in four forms:

- designing defects
- implementation defects
- configuration errors
- resource shortage

Description of the attackers and attacks

Description of the attackers

The definition of the technical capabilities of the attackers is important in order to know the nature of the threat. For example, an attacker can only receive data transmission, but it can also be introduced as a legal sensor network, and has access to all network services.

Every attacker belongs to a category

- Passer-by: with spontaneous motivation, resources and limited knowledge,
- Vandal: with resource damage motivation and limited knowledge
- Hacker: access with great motivation, curiosity and interest
- Robber: with great determination and limited resources
- Terrorist: with significant resources and a strong determination

Active attacks

The attacker tries to remove, add or change the transmission on a communication channel. An active attacker threatens the integrity and authenticity of data as well as confidentiality. In order to execute the attack, the malicious node is forced to use its energy, emitting a number of packets.

Passive attacks

The attacker only monitors the communication channels. Listening occurs when an attacker captures a node and studies traffic without altering the operation.

A passive attacker that threatens the confidentiality of data.

Table 1. Attacks in wireless sensors by layer

Layer	attack
Physical	Jamming sensor forgery
Liaison/MAC	Interrogation half-asleep
Network	Modification of control message contents Hello flooding Homing
Transport	Synchronisation flooding dis-synchronisation attacks
Application	Sensor breakdown DoS based on a track flood attack

- Jamming - Given the sensitivity of wireless media noise, a node can cause a denial of service by transmitting signals at a certain frequency.
- Hello Flooding - The network discovers protocol uses called HELLO type messages to fit into a network and to discover its neighbor nodes. In a so-called HELLO Flooding attack, an attacker will use this mechanism to saturate the network and consume energy.
- DoS - Denial of Service is defined as a malfunction of a sensor-intentioned or malicious action manner. The denial of service may not result from an attack, but a single event preventing the normal functioning of its services.

Approaches based on Elliptic Curve Cryptography

To secure any communication model, it is necessary to encrypt messages exchanged between nodes according to an agreed key management arrangement. Elliptic curves are mathematical objects (Gura *et al*., 2004) used to encrypt with shorter keys than those of public cryptography. This means faster computation and lower power consumption as well as saving of memory and bandwidth. Because of the small size of the ECC key (Blake), cryptography based on elliptic curves remains among the best security solutions for wireless sensor networks, for example ECC key (IEEE, 2001) 160-bit provides security comparable to RSA keys of 1024 bits.

Description Routing Driven Elliptic Curve (RECC)

An elliptic curve cryptographic approach based on the routing protocol GPSR (Dietrich and Dressler, 2009) (Greedy Perimeter Stateless Routing) for sensor networks.

The network consists of two types of sensors

- A small number of powerful sensors (Headers)
- Normal sensors form clusters

All communications goes through the Headers that collect the data delivered by normal nodes and route them to the base station. Two approaches to establishing key (Brad Karp and Kung, 2000), the first is centralized and the other is distributed.

- The centralized approach: Headers are responsible for the establishment and distribution of cryptographic keys.
- The distributed approach: after the creation of clusters each node is pre-loaded with all key neighbors.

Cluster Elliptic Curve Cryptography Key Management (CECKM)

This approach has a key management model based on the ECC clustering principle using an appropriate algorithm for deployment associated with a secure data transmission (Hua-Yi Lin, 2009) in wireless sensor networks. CECKM implements asymmetric key systems using ECC on sensor networks and provides dynamic key synchronization mechanism, fast and effective in network nodes without reconfiguration of all nodes when new nodes arrive or leave from the sensor network. This approach is proposed for dynamic wireless sensor networks and on a larger scale.

ECC key management based on an AVL tree

Key management should provide a key establishment between all nodes, and must work even if the network topology is not predefined. Unauthorized nodes cannot perform communication with network nodes. This approach offers management key based on AVL tree system, because in the event of a change of a node (in AVL tree), it can cause a change in a sub-tree, and the key will be also changed at the same time.

AVL Tree

The AVL tree can perform insert, delete and search in a proportional time to the height of the tree. Since each membership changes, keys that are along the path of the affected limb at the root must be changed. Following an addition of a node, the new node goes back to the roots of the tree by calculating the difference in subtree depth of each node encountered. If this difference is equal to two or both less, it balances with the proper rotation.

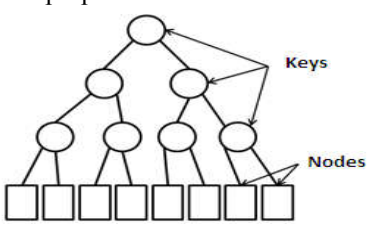

Fig. 1. The representation of keys and nodes in the tree AVL

In Figure 1, the sensors are represented by squares, and the keys are represented by circles. When messages have to be sent to all the nodes, we use the AVL tree root key because this key is known to everyone (Yi-Ying Zhang *et al*., 2008).

Comparative study of different approaches

Each approach has strengths and limitations; in the following we present a comparative study of these three approaches.

To evaluate the performance of each method, we focus on these three metrics:

- The number of ECC keys stored in each sensor.
- Energy consumption per sensor.
- The number of packets exchanged between nodes during key installation.

The following equations show how to calculate the metrics:

The size of the memory used by a sensor:

$T = (N_{CS} \times 40 \text{ bytes})$
T: Memory size
N_{CS}: number of ECC keys stored
40 bytes: the size of an ECC key

The energy consumed in the network is:

$(N_{PR} \times E_R) + (N_{PE} \times E_E)$
N_{PR}: Number of received packets
E_R: Energy to receive a packet
N_{PE}: Number of sent packets
E_E: Energy to send a packet

Energy consumption per sensor

Consumption by the Headers

CCED-C is the method where in the Header consumes more power because of its role as distributor of ECC keys. However in the AVL-KDC approach, the header does not exchange any message with the nodes of the cluster when installing keys, which accounts for low consumption.

Table 2. Average Energy Consumption by Headers

	Energy consumption per Header	consumption depends on
RECC-D	Average	Number of nodes
RECC-C	Higher	Number of nodes
CECKM	Average	Cluster size
AVL-Headers	Average	Number of nodes
AVL-KDC	Very low	Nothing

We can see in Table 2 that the AVL-KDC method is the most efficient in energy consumption, because no node participates in the management and distribution of ECC keys. In other methods nodes involved differently and consumption depends on the number of nodes in the cluster.

Energy consumption per normal sensor

Energy consumption methods CCED-D CECKM and AVL-Headers depends on the number of nodes per cluster and the number of packets exchanged during key installation.

The large number of packet exchanges between normal sensors in a cluster when installing keys, makes the most captivating CECKM consumption method of energy.

Table 3. Average Energy Consumption by normal nodes

	Energy consumption per normal node	Consumption depends on
RECC-D	*Low*	*Nothing*
RECC-C	*Low*	*Nothing*
CECKM	*Large*	*Strongly number of neighbors*
AVL-Headers	*Average*	*Nothing*
AVL-KDC	*Low*	*Nothing*

Contrary the method CECKM depends on the number of neighbors, Table 3 shows that normal sensors in the other methods do not participate in the management and distribution of keys, so there is less energy consumption compared to the CECKM method.

Comparison of the number of exchanged packets

The number of packets exchanged during key installation differs from one method to another. The simulations show that the approach to key management tree based AVL (AVL-KDC) exchanges fewer packets. However CECKM method remains a method that uses a large number of packages, because of the messages exchanged between all nodes in a cluster.

The AVL-Headers method exchanges more packages between Headers and nodes than AVL-KDC method when ECC key installation.

Tab. 4. number of exchanged packets

	Number of packets exchanged	Consumption depends on
RECC-D	*Low*	*Nothing*
RECC-C	*Low*	*Nothing*
CECKM	*Great*	*highly depending on the number of neighbors*
AVL-Headers	*Average*	*Nothing*
AVL-KDC	*Low*	*Nothing*

We see in table 4 that AVL-KDC method provides smaller communication because it exchanges fewer packets. This guarantees less key installation time and therefore safer, because when communication is prolonged, a hacker is more likely to capture and modify the keys during the exchange.

Comparison of the number of stored keys

Wireless sensor nodes are characterized by a very limited memory size of about 4KBytes for RAM and flash memory for 512Kbits for Micaz sensor, so memory is the most important constraint and each ECC key a size of 40 Bytes. Accordingly, we have focused on the number of ECC keys stored in each node type, as operated storage memory size is strongly linked to the number of stored keys. Bensaber and Boumerzoug (2011) compared the memory used for the ECC keys stored in all approaches. The following graphs show the results of comparisons. These graphs show once again that the AVL-KDC method is the least occupying memory either in normal nodes or headers.

- Number of stored keys per Header

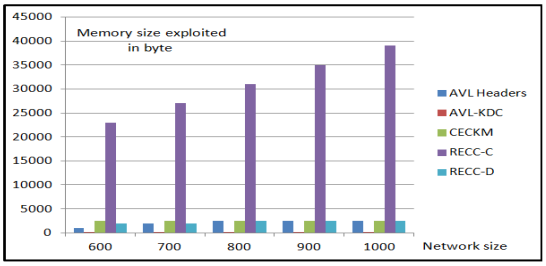

Fig. 2. Number of stored keys per Header

In the centralized approach RECC the Header saves all keys to its cluster, therefore the header uses most of his memory. AVL KDC-method is the best in terms of memory used because ECC keys are stored in the tables of the KDC server.

- Number of stored keys per normal sensor

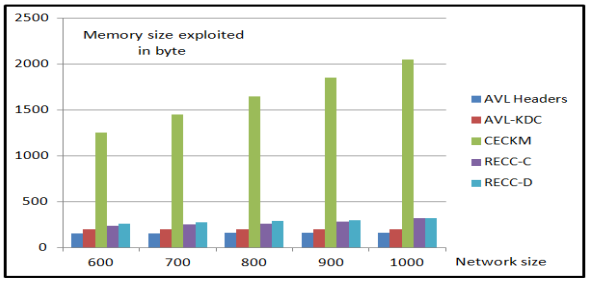

Fig. 3. Number of stored keys per normal sensor

Each node is preloaded with the keys to his neighborhood in the CECKM method which involves large memory size used for storage. Unlike CECKM method, approaches where the header or the KDC server, which ECC key, the nodes do not use their memories therefore long life network.

Conclusion

In this paper, we compared three security approaches in Wireless Sensor Networks based on Elliptic Curve Cryptography (ECC) that offers good protection, taking into account the limited sensor characteristics that directly influence the overall performance of the network, particularly safety and operating life. The comparison of the three approaches demonstrated to us the ECC key management method based on an AVL tree offers a significant gain in the storage memory and a huge reduction of packets exchanged during the key installation less calculations while ensuring better security. These approaches have been designed to reduce consumption of energy, reduce the size of storage, and while minimizing calculation and maximizing performance security. Finally, the key update method can be further improved with a more study pushed on techniques of encryption and key update, these techniques must reduce the amount of key transmitted at the start of a node, while ensuring better security.

REFERENCES

"IEEE Standard for Information Technology-Telecommunications and Information Exchange Between

Systems - Local and Metropolitan Area Networks - Specific Requirement. Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 2 : Higher-Speed Physical Layer (PHY) Extension in the 2.4 GHz Band - Corrigendum 1," IEEE Std 802.11b-1999/Cor 1-2001, pp. 0–1, 2001.

Bachir, A., Dohler, M., Watteyne, T. and Leung, K. 2010. "MAC Essentials for Wireless Sensor Networks," in Communications Surveys & Tutorials, IEEE, vol. 12, no. 2, pp. 222–248.

Bensaber, B. A. and Boumerzoug, H. 2011. "A keys management method based on an AVL tree and ECC cryptography for wireless sensor networks", International Conference on Communications, ICC 2011, ISBN 1-4244-0353-7, Glasgow, August.

Blake, I., Seroussi, G. and Smart, N. *Elliptic Curves in Cryptography*, London Mathematical Society, Lecture Note Series 265, Cambridge University Press

Boyle, P. et T. Newe, « Security Protocols for Use with Wireless Sensor Networks: A Survey of Security Architectures », in Third International Conference on Wireless and Mobile Communications, 2007. ICWMC'07, 2007, p. 54‑54.

Brad Karp, H. and Kung, T. 2000."GPSR: Greedy Perimeter Stateless Routing for Wireless Networks", Proceeding MobiCom '00 Proceedings of the 6th annual international conference on Mobile computing and networking, ISBN:1-581 13-197-6.

Dietrich, I. and Dressler, F. 2009. "On the Lifetime of Wireless Sensor Networks," in ACM Transactions on Sensor Networks (TOSN), vol. 5, no. 1, p. 5.

Dietrich, I. and Dressler, F. 2009. "On the Lifetime of Wireless Sensor Networks," in ACM Transactions on Sensor Networks (TOSN), vol. 5, no. 1, p. 5.

Gura, N., Patel, A., Wander, A., Eberle, H. and Shantz, S. C. 2004. "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," in *Proc. 6th Interna tional on Cryptographic Hardware and Embedded Systems*, Boston, MA, Aug.

Hua-Yi Lin, 2009. "High-Effect Key Management Associated With Secure Data Transmission Approaches in Sensor Networks Using a Hierarchical-based Cluster Elliptic Curve Key Agreement", ncm, pp.308-314, Fifth International Joint Conference on !NC, IMS and IDC, ISBN 978-0-7695-3769-6, Seoul, Korea.

Karl, H. and Willig, A. 2005. *Protocols and Architectures for Wireless Sensor Networks*, p.p. *200-230, John Wiley* & Sons Ltd..

Karl, H. and Willig, A. 2005. Protocols and Architectures for Wireless Sensor Networks. John Wiley & Sons.

Kuntz, R., Montavont, J. and Noël, T. 2011. "Improving the medium access in highly mobile Wireless Sensor Networks," Telecommunication Systems, pp. 1–22.

Landsiedel, O., Ghadimi, E., Duquennoy, S. and Johansson, M. 2012. "Low power, low delay : opportunistic routing meets duty cycling," in Proceedings of the 11th international conference on Information Processing in Sensor Networks (IPSN'12), (New York, NY, USA), pp. 185–196, ACM, Avril.

Marc Joye, " Introduction élémentaire à la théorie des courbes elliptiques, UCL Crypto Group Technical Report Series ", book in : *http://www.dice.ucl.ac.be/crypto/*.GC-199511 , pages (17) (73) (29-52).

Munivel, E.Dr Ajit, G.M. 2010. "Efficient Public Key Infrastructure Implementation in Wireless Sensor Networks ", International conference on Wireless Communication and Sensor Computing, ISBN 978-1-4244-5136-4, February.

Roth, D., Montavont, J. and Noel, T. 2010. "MOBINET : gestion de la mobilité à travers différents réseaux de capteurs sans fil," in 12èmes Rencontres Francophones sur les 156 bibliographie Aspects Algorithmiques de Télécommunications (AlgoTel'10)) (M. G. Potop-Butucaru and H. Rivano, eds.), (Belle Dune, France), Juin.

Yi-Ying Zhang, Wen-Çheng Yang, Kee-Bum Kim, Myong-Soon Park, 2008. "An AVL Tree-Based Dynamic Key Management in Hierarchical Wireless Sensor Network ", International Conference on Intelligent Information Hiding and Multimedia Signal Processing, ISBN 978-0-7695-3278-3, August.

****