REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE

UNIVERSITE MOHAMED BOUDIAF - M'SILA

FACULTE :DES MATHEMATIQUES ET DE L'INFORMATIQUE

DEPARTEMENT : INFORMATIQUE

N° :……

DOMAINE : MATHEMATIQUES ET INFORMATIQUE

FILIERE : INFORMATIQUE

OPTION : RESEAUX ET TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

MEMOIRE PRESENTE POUR L'OBTENTION

DU DIPLOME DE MASTER ACADEMIQUE

Par: LAGHOUEGRoumaissa

BELKAIBECH Dounia

Intitulé

Secure Data Transmission Based on Elliptic Curve Cryptography for WSN

Soutenudevant le jury composé de :

Chikouche Noureddine	Université de M'sila	Président
Mezrag Fares	Université de M'sila	Rapporteur
Lakehal Meftah	Université de M'sila	Examinateur

Année universitaire : 2019 /2020

Dedication

I dedicate this to My parents and my partner Roumaissa

Dounia

Dedication

I dedicate this work to

My dear mother and my dear father

who have never stopped, to formulate prayers to me, to support me and to help me so that I can achieve my goals,

My dear brothers and sister

To my dear sister and her husband

for their moral support and their valuable advice throughout my studies

To my dear grandfather and grandmother

who I wish them good health,

To my dear partner DOUNIA

for her understanding and her sympathy,

To my dear friends *for their help and support in times of need,*

To all my family

Roumaissa

Acknowledgements

Throughout the writing of this dissertation we have received a great deal of support and assistance and for that :

First of all, we would like to thank our supervisor Prof F.Mezrag .discursive for its teaching and guidance., thank to him so much for all your help.

we would like to thank the members of the jury for their presence, for their reading careful of our work as well as for the remarks they will make to us during this defense to improve our work.

we would like to say From the bottom of our heart a special thank you to our parents for their wise counsel and sympathetic ear. You are always there for us. Finally, we could not have completed this dissertation without the support of our friends, who provided stimulating discussions as well as happy distractions to rest our mind outside of our research.

Abstract

In recent years, wireless sensor networks have become very widespread. They're usually deployed in hostile areas, making it easier for the hacker and make them vulnerable to several attacks in which the intruder can take control of one or more nodes to disrupt the proper functioning of the network.Recently, a mutual authentication and key management scheme was proposed to secure data transmission in WSNs. In this research work, we show that this scheme has various security flaws, such as MITM attack and lack of mutual authentication between sensor nodes. Then, we propose an enhanced scheme to overcome the identified security weaknesses. Our scheme is implemented using the cryptographic library RELIC and ECMQV scheme. After a set of tests on cooja simulator, the results obtained showed that our proposal achieves good performances in terms of energy consumption, computational and communication costs. In addition, our scheme guaranties a good level of security compared to SDTS.

Keywords: WSN, Security, data transmission, attacks

RESUME´

Ces dernières années, les réseaux de capteurs sans fil sont devenus très répandus. Ils sont généralement déployés dans des zones hostiles, ce qui rend plus facile pour le pirate et de les rendre vulnérables à plusieurs attaques dans lesquelles l'intrus peut prendre le contrôle d'un ou plusieurs nœuds pour perturber le bon fonctionnement du réseau. Récemment, un système d'authentification mutuelle et de gestion des clés a été proposé pour sécuriser la transmission de données dans les WSN. Dans ce travail de recherche, nous montrons que ce système comporte diverses failles de sécurité, telles que l'attaque MITM et le manque d'authentification mutuelle entre les nœuds de capteur. Ensuite, nous proposons un plan renforcé pour surmonter les faiblesses de sécurité identifiées. Notre système est mis en œuvre à l'aide de la bibliothèque cryptographique RELIC et du système ECMQV. Après une série de tests sur le simulateur cooja, les résultats obtenus ont montré que notre proposition réalise de bonnes performances en termes de consommation d'énergie, de calcul et de coûts de communication. En outre, notre régime garantit un bon niveau de sécurité par rapport à SDTS.

نبذة مختصرة

في السنوات الأخيرة ، أصبحت شبكات الاستشعار اللاسلكية شائعة جدًا. وعادة ما يتم نشرها في مناطق معادية ، مما يسهل على المتسلل ويجعلها عرضة لهجمات متعددة يمكن للمتطفل من خلالها السيطرة على عقد أو أكثر لتعطيل الأداء السليم للشبكة. في الآونة الأخيرة ، تم اقتراح نظام مصادقة متبادلة وإدارة المفاتيح لتأمين نقل البيانات في شبكات WSN. في هذا العمل البحثي ، أظهرنا أن هذا النظام به عيوب أمنية مختلفة ، مثل هجوم MITM وعدم وجود مصادقة متبادلة بين عقد الاستشعار. كما اقترحنا خطة معززة للتغلب على نقاط الضعف الأمنية المحددة. يتم تنفيذ نظامنا باستخدام مكتبة التشفير RELIC ونظام ECMQV. بعد سلسلة من الاختبارات على جهاز محاكاة cooja ، أظهرت النتائج التي تم الحصول عليها أن اقتراحنا يحقق أداءً جيدًا من حيث استهلاك الطاقة والحساب وتكاليف الاتصال. بالإضافة إلى ذلك ، يضمن نظامنا مستوى جيدًا من الأمان مقارنة بـ SDTS.

Table of Contents

List of Figures

List of Tables

General Introduction

The "Internet of Things" (IoT) isn't the "publicity" or a "popular expression" anymore, Iot currently has the ability to change our world. it provides in a diverse range of applications, such as tracking, homes, make healthcare, remote monitoring, localization, event-reporting [1] and other areas that affect people and the environment smarter, This reduces costs and makes life more comfortable.

As IoT devices include wireless sensors, WSNs have a crucial effect on the IoT. WSNs are networks of small, battery-powered, memory-constraint devices, limited processing speed named sensor nodes, which have the capability of wireless communication over a restricted area. The purpose of this is to monitor a geographical area, and sometimes to act on it. Examples include the detection of forest fires, the surveillance of a battlefield, the surveillance of vehicle movements in hostile zones, the surveillance of infrastructures. Treatment for patients etc. Typically a wireless sensor network contains hundreds of thousands of sensor nodes [2] . The sensors are placed more or less randomly (for example by dropping from a helicopter) in environments that may be dangerous, where any human intervention after the deployment of the sensor nodes is excluded, the network must, therefore, be self-managed. So that the sensor nodes work in a cooperative, the information collected is shared between them over the air. Be that as it may, the arrangement of WSNs in unattended conditions makes the sensor hubs defenseless against different security attacks [3] .

At present time, most of the research on WSNs has concentrated [4]to secure data transmission in WSNs and prevents information leakage. One of the most severe security threats in WSNs is security compromise of sensor nodes due to their lack of tamper resistance [3] . In WSNs, the attacker could compromise multiple nodes to obtain their carried keying materials and control them, and thus is able to intercept data transmitted through these node thereafter. Harbi et al propose a lightweight security mechanism named Secure Data Transmission Scheme (SDTS). aims to secure data transmission in WSNs. by using Elliptic Curve Cryptography (ECC) .[5]

In this work, we show that this scheme has various security flaws, such as MITM attack and lack of mutual authentication. Then, we propose an enhanced scheme to overcome the identified security weaknesses. Our scheme is implemented using the cryptographic library RELIC and ECMQV scheme. After a set of tests on cooja simulator, the results obtained showed that our proposal achieves good performances in terms of energy consumption, computational and communication cost. In addition, our scheme guaranties a good level of security compared to SDTS scheme.

This research work is arranged as follows:

Chapter 1 :

Overview of wireless sensor networks (WSNs). Starting with Applications of WSN like (Environmental Monitoring, Military, health care,...,etc). Description of the main concepts related to wireless sensor networks such as WSN Architecture, Challenges in WSN, Sensor node Architecture With just a few examples, and Operating systems.

Chapter 2 :

This chapter focuses on Security requirements in WSN and Classification of attacks, as well as a classification of the different types of Cryptography.

Chapter 3:

lists the basic Overview of in the paper Harbi etal schemes and its weakness, After that, we proposed a security scheme an improvement to an approach already presented in this chapter with the presentation of the simulation results. We end our paper with a general conclusion proposed security scheme.

Chapter 1
Wireless Sensor Networks (WSNs)

Chapter 1 Wireless Sensor Networks (WSNs)

1.1 Introduction

Wireless Sensor Networks (WSNs) have been widely used in different applications such as environmental monitors, military, healthcare and industry[6].WSNs are currently considered one of the technologies that attracted the attention of researchers, which consist of large number oftiny devices called sensor nodes deployed deterministically by hand or randomly in the target environment.These sensor nodes can exchange data between them without using a preexisting and fixed network infrastructure or centralized control. Moreover, each one communicates directly with other nodes that are within its transmission range. To note,the Base Station(BS) represents a downstream of all data coming from sensor nodes. However, sensor nodes are constrained in terms of their storage space, battery power, and computational capability. In this chapter, we will give an overview about WSN by introducing some description of their general concepts, including the sensor node and WSN architectures, domains application, challenges in WSN and operating systems dedicated to WSN. Finally, we will conclude this chapter by giving a conclusion.

1.2 Sensor node architecture

A sensor node consists of four basic units, including a sensing unit, a processing unit, a communication unit and a power unit (battery). The details is described as follows:

1.2.1 Sensing unit

This unit is composed of two subunits: a sensor and an Analog to Digital Converter (ADC). The sensor observes the physically phenomena and then generates an analog signal based on the observed phenomenon. The ADC conversan analogsignal into a digital signal which is delivered to the processing unit for further analysis.

1.2.2 Processing unit

It consists usually a micro-processor (micro-controller)with a small memory. It operateswith an operating system specially designed for sensor node. Which provides an intelligent control to the sensor node.

1.2.3 Communication Unit

This unit is responsible for carrying out all data transmissions and receptions over a radio channel.

1.2.4 Power unit

The power unit consists of a battery for supplying power to drive all other units in the sensor node. It is worth noting that a battery is limited and generally non replaceable. This often makes an energy the most precious resource of a sensors network, because it directly influences the lifetime of sensor nodes and therefore of the entire network.

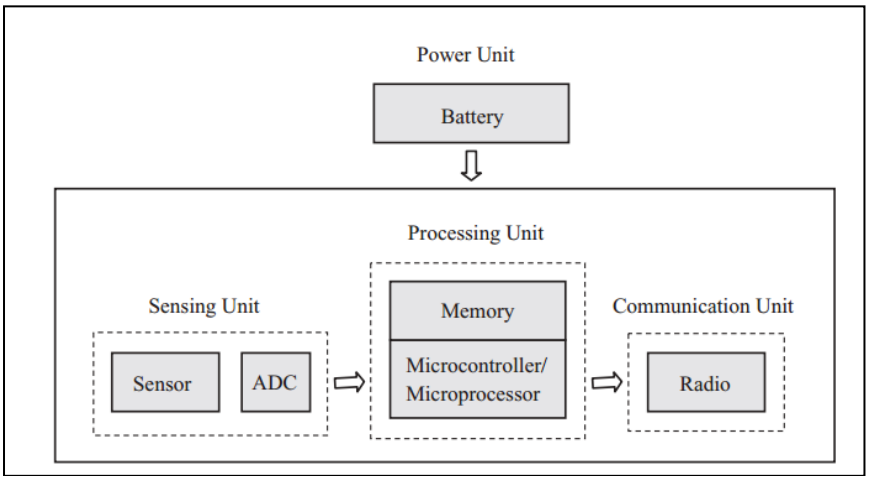

FIGURE 1*Sensor node architecture[7]*

1.3 Example of Sensor nodes

There are several commercial platforms of wireless sensors, among the most famous: WiSMote and Tmote Sky (Figure 2).The table1 presents the characteristics of platforms.

TABLE 1 CHARACTERISTICS OF WISMOTE AND TMOTE SKY PLATFORMS

Properties	WiSMote	Tmote Sky
Microcontroller	TI MSP430F5437x	MSP430 F1611
Frequency (MHz)	16	3.9
RAM (KB)	16	10
ROM(KB)	256	48
Radio interface	CC2520	CC2420
Battery	2AA	2AA

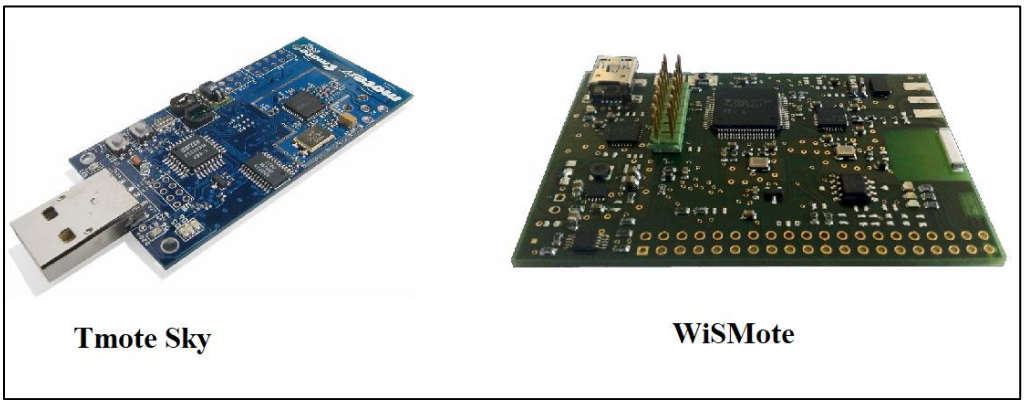

FIGURE 2 EXAMPLE OF SENSOR NODES

1.4 WSN Architecture

Sensor nodes are usually scattered in a sensing region as shown in Figure 3. Each node can gather data and route them to BS by a wireless multi-hop communication. The BS can be connected to the network user via an Internet or satellite[8].

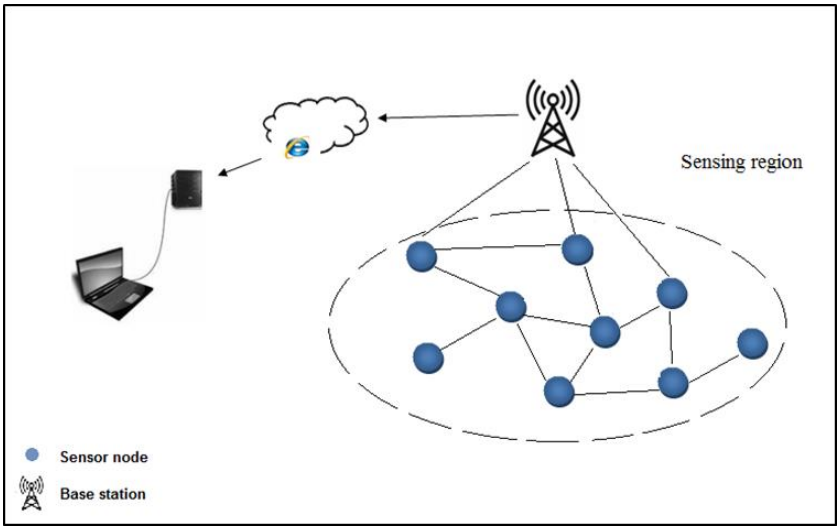

FIGURE 3 FLAT-BASED ARCHITECTURE

In cluster-based network, sensor nodes are organized into clusters, where the nodes of same cluster send message packets to Cluster Head (CH). This latter accomplish the task of transmitting data packets to BS. In this architecture, signals from node have to cover less distance as compared to flat-based architecture that saves energy consumption in the network.

Role of cluster head can be switched among members of group. Figure 4 shows cluster-based architecture.

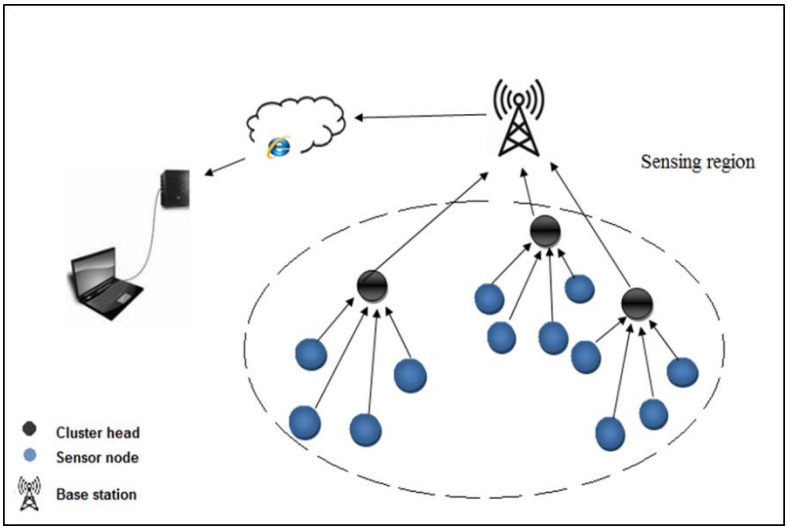

FIGURE 4 CLUSTER-BASED ARCHITECTURE

1.5 WSN applications and challenges

This section introduces several sensor network applications(Figure 5)[9]. As well as the challenges of WSN.

1.5.1 Environmental Monitoring

The sensor networks can monitor several environmental parameters such as underground water level, barometric pressure, ambient temperature, atmospheric humidity, wind direction, wind speed and rainfall and provide various convenient services for end users who can manage the data via a website from long-distance or applications in console terminal.

1.5.2 Military Applications

There is always a threat of being attacked by enemies. So, the use of these cheap sensor nodes will help to reduce the loss. For example to monitor all movements (friends or enemies), or to analyze the terrain before sending troops (detection of chemical agents, biological or radiation). This will further help to improve the troop readiness and decrease the reaction time.

1.5.3 Healthcare Applications

Wireless sensor networks are also applied in the health care fields for, for example, monitoring blood sugar, monitoring vital organs or early detection of cancer. On the other hand these networks can detect abnormal behaviors (fall of bed, shock, cry, etc) in disabled or elderly people, and therefore permanent monitoring of patients.

1.5.4 Industrial Process Control

In industry, WSNs can be used to monitor manufacturing processes or the condition of manufacturing equipment For example, wireless sensors can be instrumented to production and assembly lines to monitor and control production processes. Chemical plants or oil refiners can use sensors to monitor the condition of their miles of pipelines.

1.5.5 security and surveillance

The application of sensor networks in the field of security and surveillance can considerably reduce the financial expenditure devoted to securing places and human beings. Thus, the integration of the sensors in large structures such as bridges or buildings will help to detect cracks and alterations in the structure following an earthquake or the aging of the structure. The deployment of a network of motion detection sensors can constitute an alarm system which will be used to detect intrusions into a surveillance zone.

1.5.6 Home Intelligence

Allow a user to control home appliances locally or remotely. such as: the light goes out and the music stops when the room is empty, the air conditioning and heating adjust according to the multiple measurement points, the alarm is triggered by the anti-intrusion sensor when a stranger wants enter the house.

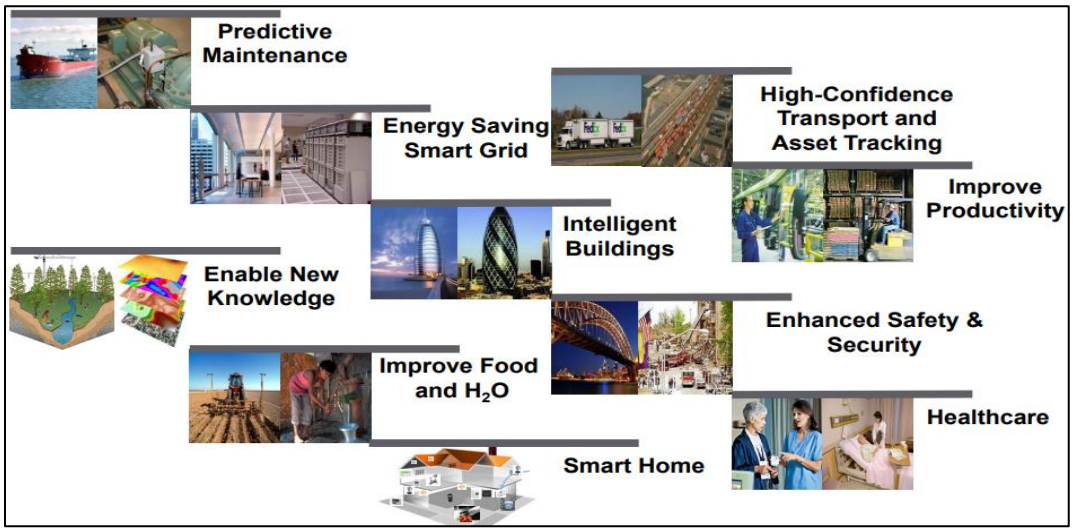

FIGURE 5 WSN APPLICATIONS

1.5.7 Challenges in WSN

The main constraints imposed on sensor networks are summarized in the following points [10]

- ✓ **Energy consumption**

Energy conservation is one of the major issues in the sensors networks. In fact, recharging energy sources is often too costly and sometimes impossible. Moreover, the nature of the network can sometimes lead to additional dissipation of energy. Thus, the lifetime of the network depends on the lifetime of the batteries of sensor nodes. Therefore, it is necessary that the sensors save as much energy as possible in order to be able to operate.

- ✓ **Network scalability**

The number of deployed sensor nodes can reach one million. Such a large number of sensor nodes generates intensive flows directed towards the base station. The latter must absolutely be equipped

with sufficient memory space to store the data received. Effective data aggregation techniques must be put in place to mitigate unnecessary replication of messages.

- ✓ **Fault tolerance**

Some sensor nodes can generate errors or stop working due to a lack of energy, a physical problem. These problems do not have to the rest of the network, following the principle of fault tolerance, which is the ability to maintain network functionality without any interruptions caused by hardware or software incidents.

- ✓ **The environment**

Sensor nodes are often deployed on masse in hard-to-reach places, such as battlefields, inside large machines, at the bottom of an ocean, in biologically or chemically soiled fields. Therefore, it becomes essential to ensure the proper functioning of the network without monitoring it.

- ✓ **The materiality constraint**

The main materiality constraint is the size of the sensor, which must be fairly small, as well as the resistance of the sensor to likely breakage and accidents.

1.6 Operating systems dedicated to wireless sensor networks

Due to resource constrained of sensor device especially when it comes to the low memory space, the modest computational capacity and the limited energy, it was inevitable to develop operating systems that are dedicated to sensor device. TinyOS (tiny operating system) and Contiki are among the most popular operating systems. In the table below, we compare Contiki-OS and TinyOS according to several criteria[11]:

TABLE 2COMPARISON OF TINYOS AND CONTIKI

	Model of programming	Support real-time apps	Language	Simulator
TinyOS	Oriented events	No	NesC	TOSSIM
Contiki	Based-events & Protothreading	No	C	Cooja

1.7 Contiki-OS

Contiki-OS is an operating system for networked, memory-constrained systems with a focus on low-power wireless Internet of Things devices. It is open-source software released under a BSD license. Moreover, Contiki-OS provides multitasking and a built-in Internet Protocol Suite (TCP/IP stack), yet needs only about 10 kilobytes of random-access memory (RAM) and 30 kilobytes of read-only memory (ROM). Therefore, a full system, including a graphical user interface, needs about 30 kilobytes of RAM. Contiki-OS includes a network simulator called Cooja, which simulates networks of Contiki nodes[12].

1.7.1 Cooja simulator

- Cooja is the Contiki network simulator. It is Java Based application with a graphical userinterface GUI based on Java's standard Swing [13] , To speed up development and testing ofContiki applications.
- It can simulate large and small networks of Contiki motes
- It allows developers to test their code and systems before running it on the real target hardware, to estimate power consumptions of nodes in simulations or to show radio transmissions and receptions.

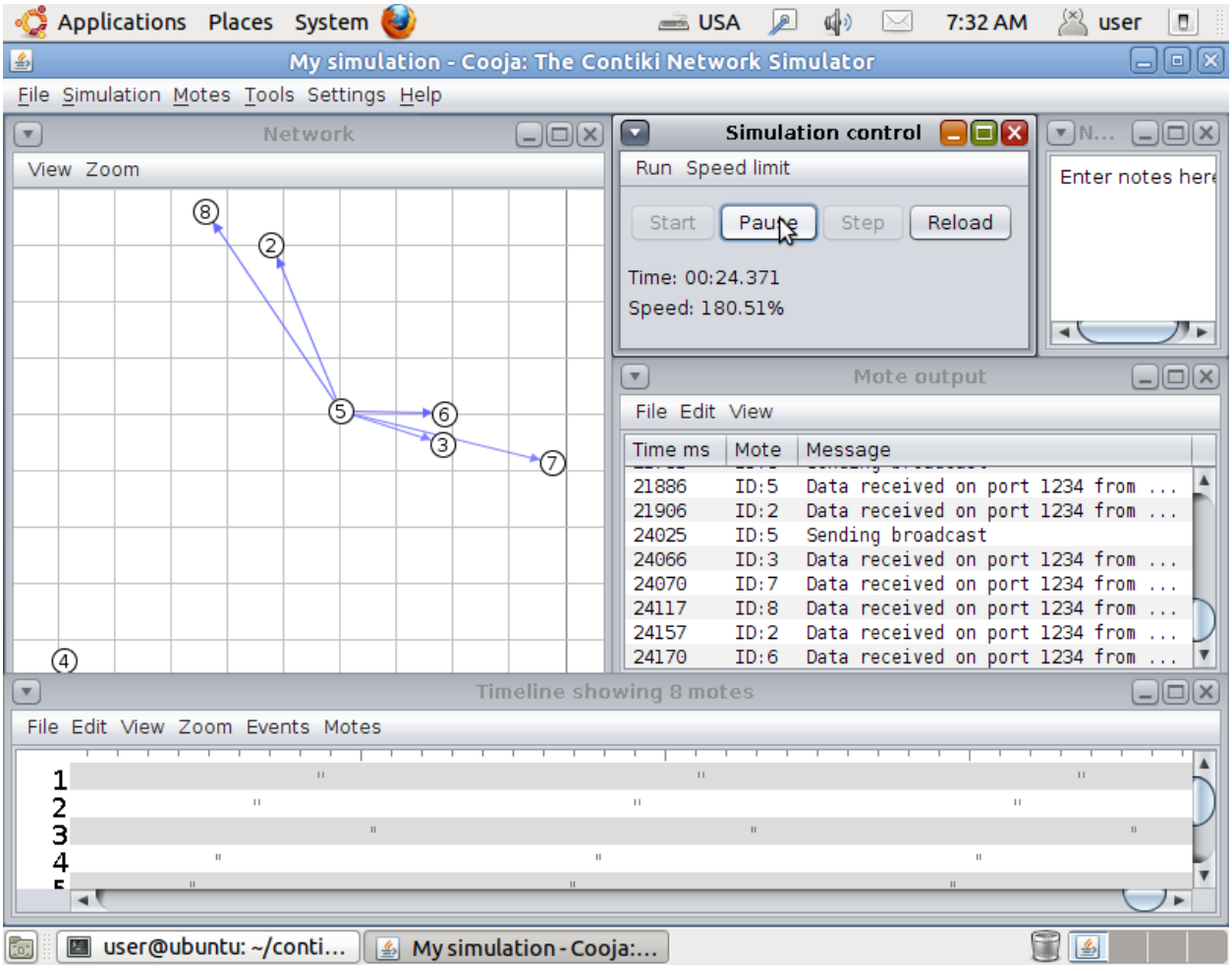

FIGURE 6 COOJA SIMULATOR

1.8 Conclusion

In this chapter, we have described the main concepts related to wireless sensor networks such as: architecture, featured applications, main features and limitations

Chapter 2
Security in Wireless Sensor Networks

Chapter 2 Security in Wireless Sensor Networks

2.1 Introduction

Recently, the use of sensors network has increased even more rapidly in all areas with the introduction of miniaturization technology. As a result, there has been mass production of sensor nodes with poor hardware, which is generally not tamper-proof. Therefore, sensor nodes can easily be threatened by a malicious nodes or a powerful pc. In this chapter, we present the fundamental aspects of the security of wireless sensor networks. We also present the basic solutions, which are proposed in the literature to meet the needs in terms of security.

2.2 Security requirements in Wireless Sensor Networks

Security solutions intended for sensor networks must fulfill one or more security requirements.[14]

2.2.1 Authentication

It can happen that an attacker not only causes the modification of the packets he intercepts but also, he can forge and inject spoofed packets into the network. In such a case, the sensor node must be able to verify the validity of the identifiers of the data source nodes which reach it.

2.2.2 Confidentiality

Confidentiality is a very important point in the wireless communication of WSNs, it refers to keep sent data secret by encrypting the data.

2.2.3 Integrity

This security requirement ensures that the sent data are received without any alteration by an adversary.

2.2.4 The freshness

An adversary can violate this security requirement, by repeatedly replaying old messages. Therefore, the messages transmitted should be recent and have not been replayed.

2.2.5 Availability

Even in the event that the sensor network is targeted by attacks, the network should resist as much as possible and preserve the availability of its resources and services.

2.3 Classification of attacks in Wireless Sensor Networks

Attacks against sensor networks can be classified into the following categories [15, 16]

2.3.1 External attack *VS* Internal attack:

External attacks occur through nodes that are not deployed inside the network and that are not allowed to participate in the network, while internal attacks occur through malicious internal nodes. The latter category is the most severe type of threat that can disrupt the proper functioning of the network, and is difficult to detect.

2.3.2 Passive attack *VS* Active attack

The objective of the passive attack is to obtain information without any modification on the exchange. Usually, the attacker is limited to listening to the traffic exchanged. It collects a large volume of data and performs a data analysis to extract secret information, or knowledge of important nodes in the network (Cluster-Head). This extracted information can then be used by the attacker for malicious purposes. In an active attack, the attacker attempts to exploit the security vulnerabilities of the network to launch various attacks in order to modify the data or disrupt the proper functioning of the network.

2.3.3 Laptop-class attack *VS* Mote-class attack

The mote-class attack occurs through a sensor node. In other words, the attack device is of the same type of material as the sensor nodes which should be attacked. On the other hand, in the laptop-class attack, the opponent uses a device which is superior to the sensor nodes which should be attacked in terms of computing power and transmission power.

2.4 Attacks against sensor networks

2.4.1 Eavesdropping

In this case adversary is only charged by the listening secretly to a private conversation. However, in the paradigm of WSN, eavesdropping is an operation to learn the “aggregate data” that is being collected by the entire network.[17]

2.4.2 Man-in-the-Middle Attack

The attacker intrudes into the network and makes an effort to establish an independent connection between a set of nodes and the sink node. The nodes in the network are unaware that the entire flow control is being handled by the attacker. [18]

2.4.3 Sinkhole Attack

In a sinkhole attack, the adversary impersonates a BS and attracts the whole of traffic to a node or a set of nodes[19]

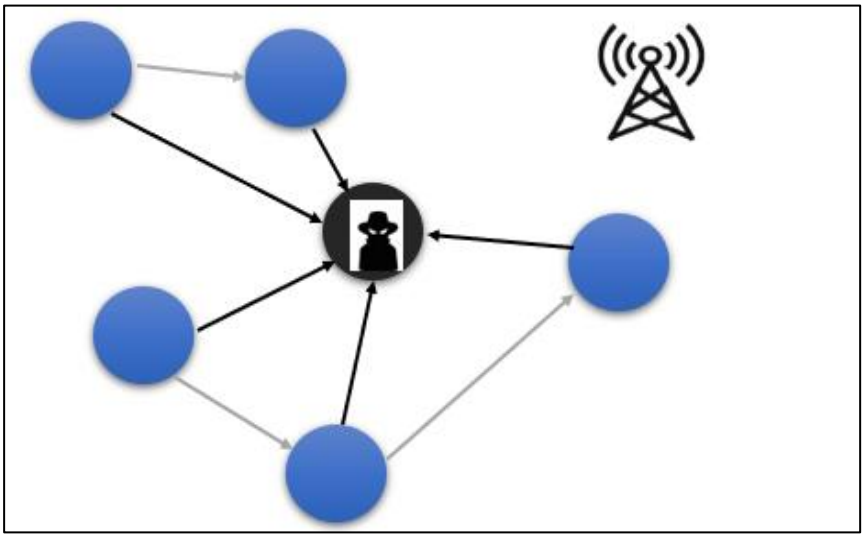

FIGURE 7 SINKHOLE ATTACK

2.4.4 Sybil Attack

This type of attack poses a serious threat to routing mechanisms in WSN. Sybil is an impersonation attack in which a malicious node masquerades as a set of nodes by claiming false identities, or generating new identities in the worst case[19]

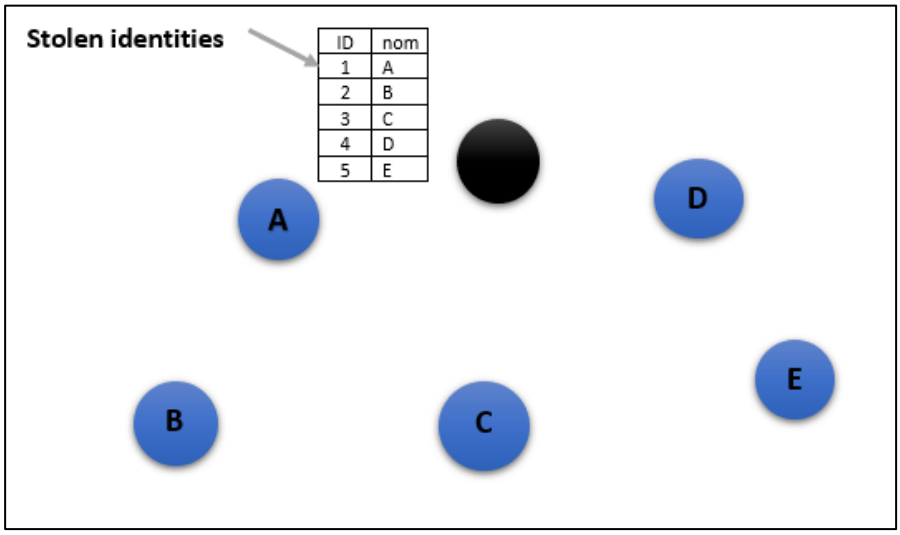

FIGURE 8 SYBIL ATTACK

2.4.5 Wormhole attacks

The principle of this attack is that the malicious nodes dispersed in the network collaborate together via virtual tunnels to undertake an organized attack. Thus, an attacker collects the data arising from the nodes of his neighborhood to reintroduce them in another area of the network, where there is another attacker.[19]

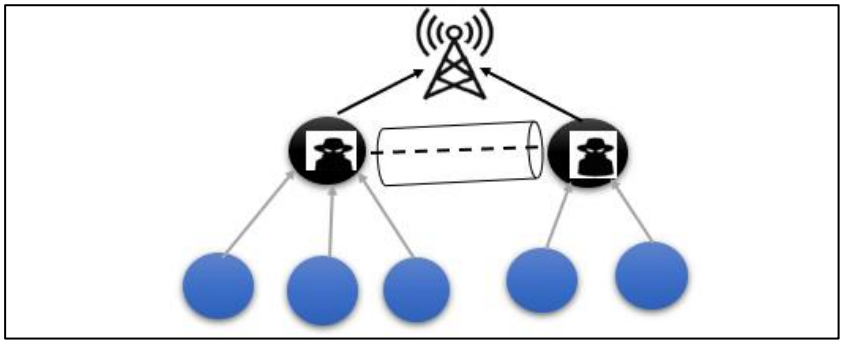

FIGURE 9 WORMHOLE ATTACK

2.4.6 Hello Flood attacks

The aim of this attack is to consume the energy of the nodes and prevent their messages from being exchanged. As the malicious node broadcasts a Hello message in the network using a large transmission energy. Therefore, all nodes that receive the message will try to forward their packets through the malicious node.[19]

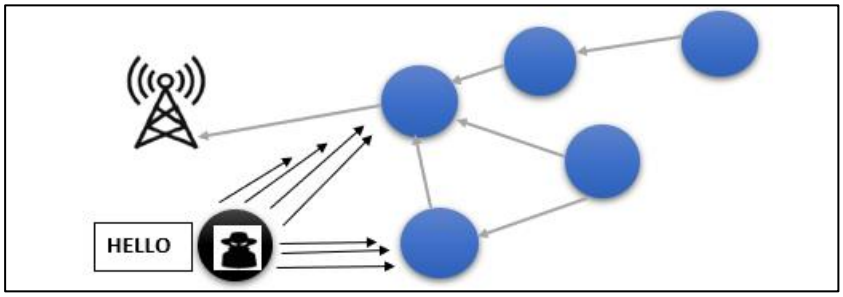

FIGURE 10 HELLO FLOOD ATTACK

2.5 Cryptography [5]

Cryptography is a fundamental security discipline that aims to protect messages by ensuring confidentiality, authenticity, and integrity. To do this, it requires the employment of an encryption and decryption algorithm which in turn uses secrets or keys for the encryption / decryption of messages.

2.5.1 Symmetric encryption

In symmetric cryptography we use a single key called the secret key or the symmetric key for encryption and decryption process.

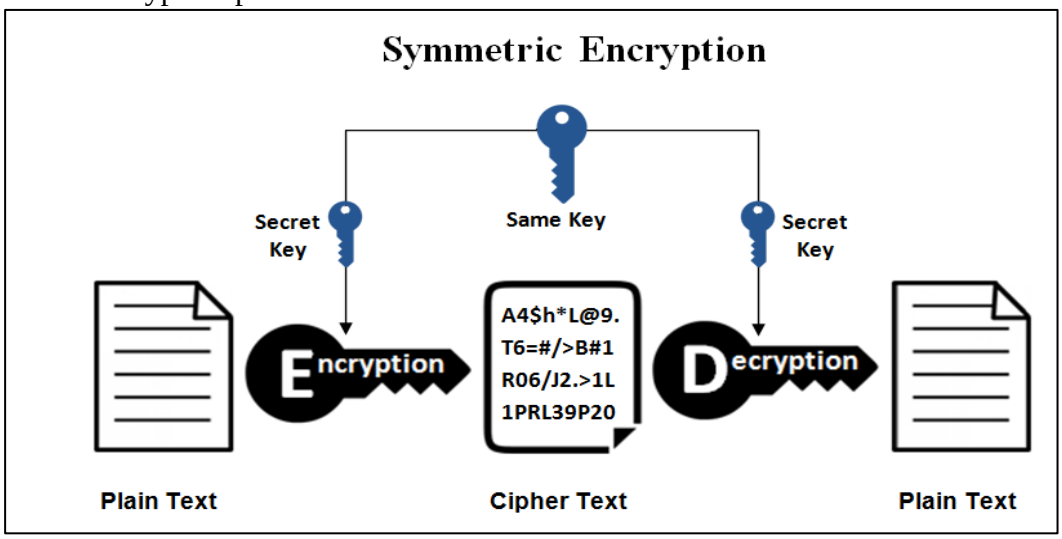

FIGURE 11 SYMMETRIC ENCRYPTION

2.5.2 Asymmetrical encryption

Asymmetrical cryptography, or public key cryptography, is an encryption method that is based on the use of two types of keys for each entity: a public key and a private (secret) key for encryption and decryption respectively.

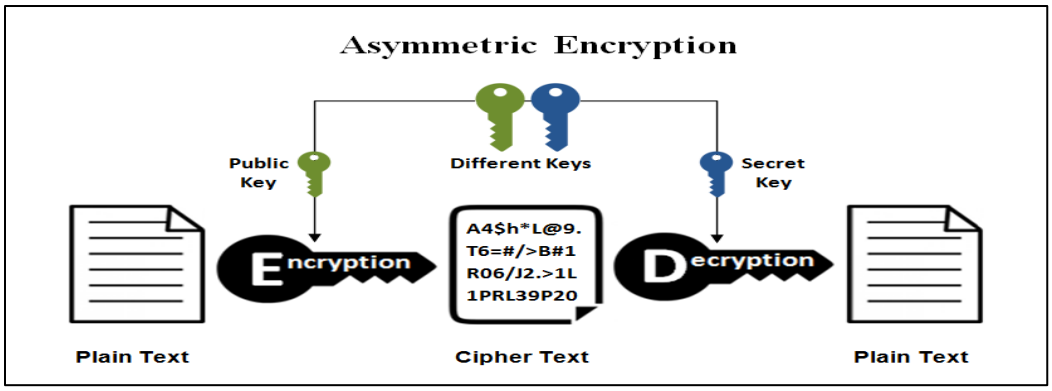

FIGURE 12 ASYMMETRICAL ENCRYPTION

2.5.3 Hash function

This function is used to check the integrity of transmitted messages.The sender uses the hash function to create the fingerprint of the message to be transmitted, then transmits the message and the fingerprint to the receiver. On receipt of the message, the receiver calculates the fingerprint of

the message received and compares it to the initial fingerprint. If the two fingerprints match, then the message could not be altered.

2.5.4 Message Authentication Codes (MAC)

A Message Authentication Code (MAC) is the result of a one-way hash function dependent on a symmetric key. At the same time, it guarantees the integrity and authentication of messages such that the adversary can neither send a message nor modify a message sent by a real transmitter

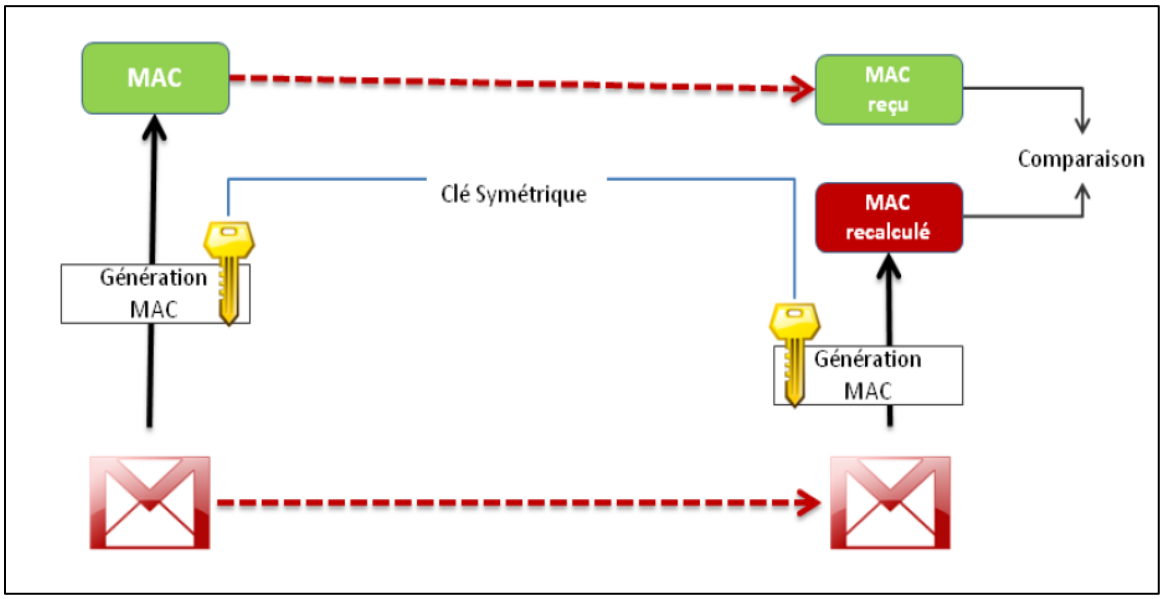

FIGURE 13 MESSAGE AUTHENTICATION CODES (MAC)

2.5.5 RSA Cryptosystem

RSA is among the most cryptographic algorithms]. The latter is invented by Rivest, Shamir and Adelman in 1978 and it is based on the difficulty of factorizing large numbers. It was so successful that today is the RSA public key algorithm is the most used in the world.

- ✓ **RSA Encryption**
  - Suppose the sender wish to send some text message to someone whose public key is (n, e).
  - The sender then represents the plaintext as a series of numbers less than n.
  - To encrypt the first plaintext m, which is a number modulo n. The encryption process is simple mathematical step as

$$C = m^e \bmod n$$

✓ **RSA Decryption**

- The decryption process for RSA is also very straightforward. Suppose that the receiver of public-key pair (n, e) has received a cipher text C.
- Receiver raises C to the power of his private key d. The result modulo n will be the plaintext m

$$\mathbf{m = C^d \bmod n}$$

2.5.6 Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptosystemis a public key cryptographic approach based on mathematical aspects of elliptic curves that satisfy the equation 1[20]. Figure8 illustrates two examples of elliptical curves. ECC can be used for public key operations such as key exchange on a public channel, and asymmetric encryptions.ECC has attracted muchattention as a means of security for WSN due to the smallsize of the ECC key compared to the RSA key.

$$f(x) = x^3 + ax + b, \Delta = 4a^3 + 27b2 \neq 0. \quad (1)$$

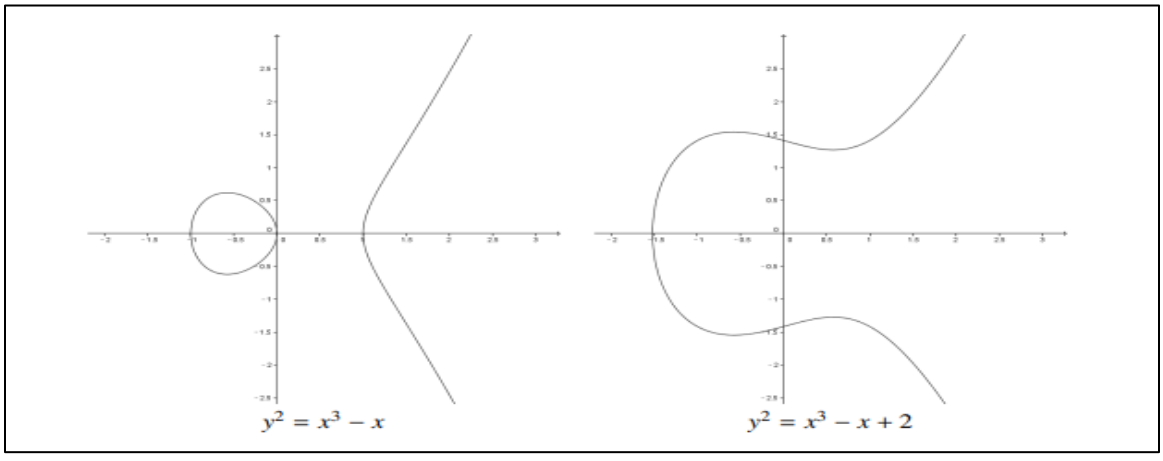

FIGURE 14EXAMPLES OF ELLIPTICAL CURVES[21]

2.5.6.1 Comparing ECC vs RSA

Studies of the RSA and ECC cryptography systems concluded that elliptical curves require shorter keys than RSA. However, the use of small keys confers a great deal of benefits calculations are faster, overall electricity consumption is reduced, and memory space is reduced Unlike RSA, elliptical curves are faster for private operations.Table 3, Figure 15, Figure 15 and Figure 16shows the comparison between ECC and RSA and how that elliptical curves are faster than RSA for private operations .

TABLE 3 ECC AND RSA COMPARISON[22]

RSA key size	ECC key size
1024	160
3072	256
7680	384
15360	512

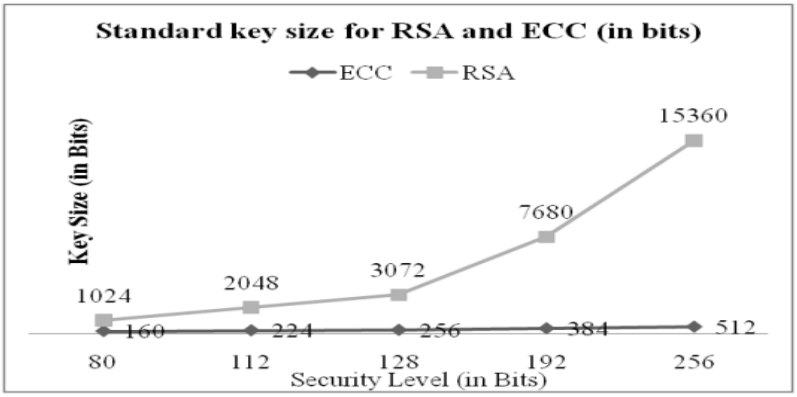

FIGURE 16 COMPARABLE SECURITY BIT LEVEL FOR CRYPTOGRAPHY KEY LENGTH[23]

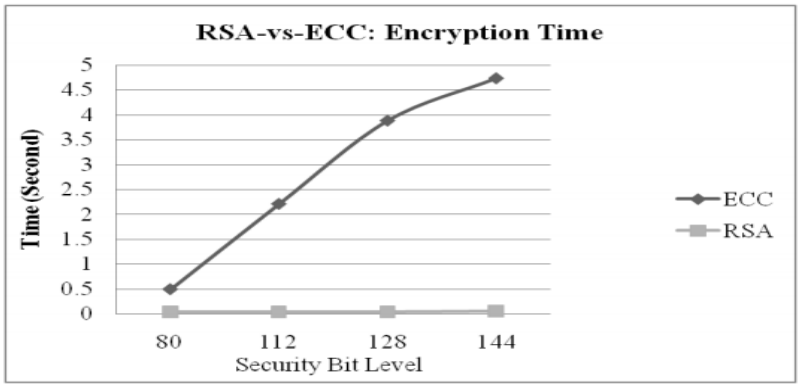

FIGURE 17 8 BITS - ENCRYPTION TIME (IN SECONDS)[23]

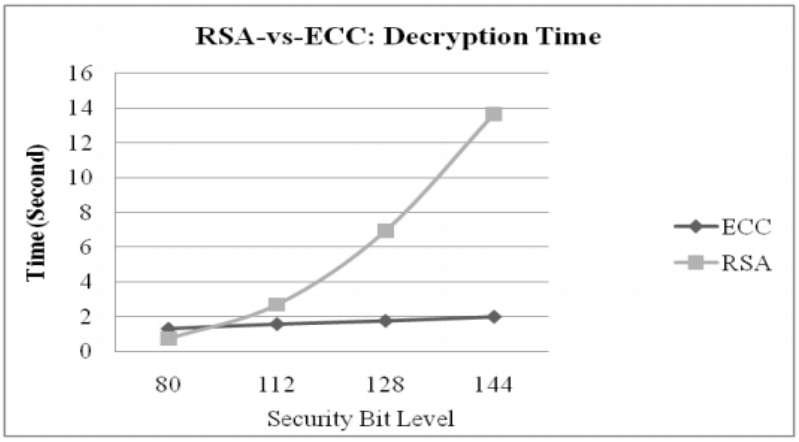

FIGURE 18 8 BITS - DECRYPTION TIME (IN SECONDS)[23]

2.5.6.2 Elliptic Curve Discrete Logarithm Problem (ECDLP)

Let P, Q ∈ E (p) such that Q = kP, then, it is difficult to determine k given P and Q. This problem is called the elliptic curve discrete logarithm problem (ECDLP) [24].

2.5.6.3 Elliptic Curve Diffie-Hellman (ECDH)

ECDH [25]is a key exchange mechanism basedon elliptic curves helping two nodes to compute a sharedsecret key that can be used for symmetrickey cryptography.We suppose two sensor nodes A and B, each having a pair of private-public keys, and want to compute a shared secret key SK. First, A and B exchange the public keys PU_A and PU_B. Then, A computes (PR_A* PU_B). B computes (PR_B* PU_A). It worth noting that PR_A andPR_B are private keys for sensor nodes A and B, respectively.

PU_A =PRA * G and PUA=PRA * G, where G is the generator point on the elliptic curve. Thus, PRA* PU_B = PR_A* PR_B * G = PR_B* PU_A. A and B have the same PR_A* PR_B * G which is considered as shared secret key between A and B.

2.5.6.4 Elliptic Curve Menezes-Qu-Vanstone Scheme (ECMQV)

Elliptic Curve Menezes Qu Vanstone Algorithm (MQV): The MQV addresses issues in the Dh key agreement algorithm. ECMQV has all the security attributes desired in a key agreement protocol, making it trusted and secure. ECMQV also has many desirable performance attributes, including that the dominant computational steps are not intensive, is role-symmetric. The ECMQV key agreement method is used to establish a shared secret between two nodes that can be used for symmetric-key cryptography. We suppose two sensor nodes A and B. who already possess trusted copies of each other's public keys. As both sides have possesses a long-term key pair (A, a) and (B,b). With A, B Long-term public keys and a,b Long-term private (secret) keys. The steps of ECMQV protocol is shown in the table :

TABLE 4 THE STIPS OF ECMQV PROTOCOL

step	Operation
1	**A** generates a key pair (X,x) by generating randomly x and calculating X where X=xP with P a point on an elliptic curve.
2	**B**generates a key pair (Y,y) in the same way as A
3	**A** calculates Sa = x+$\bar{X}$a modulo n and sends to B
4	**B** calculates Sb = y +$\bar{Y}$b modulo n and sends to A
5	**A** calculates SK=h.Sa(Y+$\bar{Y}$B) and B calculates SK=h.Sb(X+$\bar{X}$A) where h is the cofactor

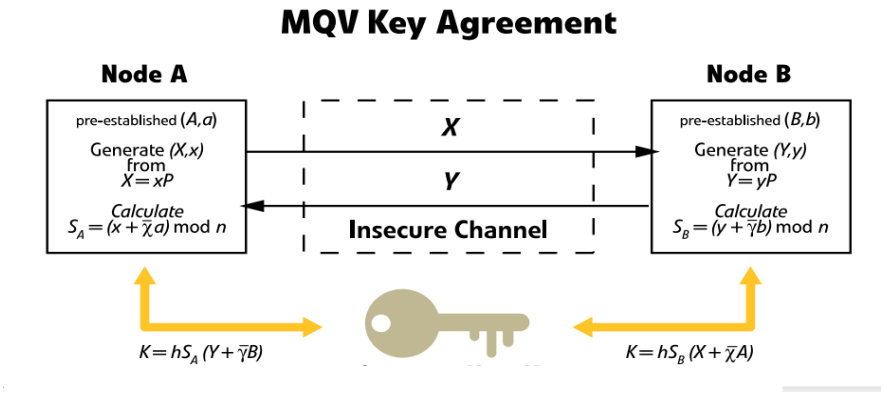

FIGURE 19ECMQV PROTOCOL [26]

TABLE 5 ECMQV NOTATIONS

Symbol	Operation
A, B	Long-term public keys
a, b	Long-term private (secret) keys
X, Y	Ephemeral public keys
x, y	Ephemeral private (secret) keys
h	h = 1/n|E(Fp)| where E(Fp) is the order ofthe elliptic curve *E* and *n* is the order of the base pointP.
$\bar{X}, \bar{Y}$	The integers derived from the *X,Y* public keys

2.5.7 CRYPTOGRAPHY LIBRARY

There exist numerous cryptography library encompassing multitudes of encryption algorithms which can be implemented for encryption of different messages in contiki [27]. The most prominent cryptography library is Relic.

2.5.7.1 RELIC toolkit

RELIC is a modern cryptographic meta-toolkit with emphasis on efficiency and flexibility. RELIC can be used to build efficient and usable cryptographic toolkits tailored for specific security levels and algorithmic choices

The different algorithms implemented by the "RELIC toolKit " are as per the following [28]:

- Multiple-precision integer arithmetic
- Bilinear maps and extensions fields relate to bilinear maps
- Elliptic curves:
    - Over prime fields
    - Over binary fields
- Cryptographic protocols
- Prime and Binary field arithmetic

Cryptographic protocols implemented by RELIC[30] :

- ECDSA
- RSA
- ECIES
- ECDH
- ECMQV

2.6 Conclusion

In this chapter we have cited the most important notions in the security of wireless sensor networks without forgetting the most common attacks.

Chapter 3

Secure Data Transmission Based on Elliptic Curve Cryptography for WSN

Chapter 3 Secure Data Transmission Based on EllipticCurve Cryptography for WSN

3.1 Introduction

In this chapter, we present Secure data transmission invented by Harbi and al then we propose a secure version of SDTS scheme. The idea is to incorporate into the new scheme that takes into account, on the one hand, the limited resources of sensor nodes and, on the other hand, dealing with attacks that are frequently conducted against the SDTS schemes.

3.2 Overview of SDTS scheme

Secure data transmission in WSN is considered as a challenging task facing this type of network. Sensor nodes deployment in open areas makes WSN vulnerable to several attacks that can adversely affect its own functioning. To address this challenge, Harbi et al[5] proposed a secure scheme called Secure Data Transmission Scheme (SDTS) which improves communication security in cluster-based WSN and prevents information leakage. SDTS is based on Elliptic Curve Cryptography and achieves several security requirements including confidentiality, integrity and authentication. The authors consider that the network consists of a single BS and a large number of homogenous sensor nodes. The BS is assumed to be a powerful and reliable device. To achieve the energy-efficient and decrease the network overhead, sensor nodes are grouped into clusters. Each one has a CH and several cluster members (CMs). The CH aggregates sensed data from their cluster's members (CMs) and send it to the BS directly. Figure 1 shows the network architecture of SDTS.

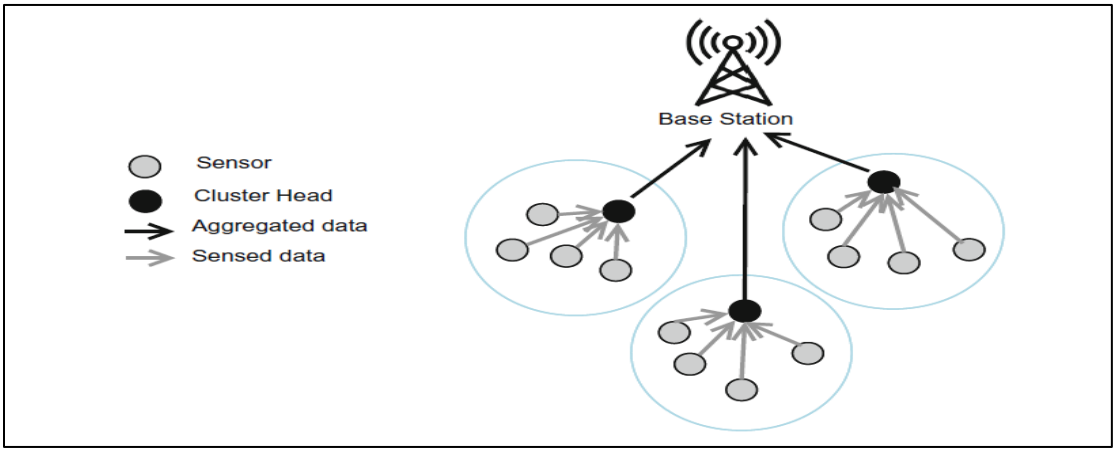

FIGURE 20 ***NETWORK ARCHITECTURE OF SDTS***

3.2.1 Notations

The notations used in this chapter are listed in as follow

TABLE 6 NOTATIONS USED

Notation	***Description***
BS CH CM	Base station, Cluster head, Cluster member
G	Generator point
P	Ephemeral public key
S	Ephemeral private key
Q	Long-term public key
D	Long-term private key
Sa	Implicit signature
SK	shared secret key
PK	Ciphered secret key
GK	Global key
ci	Encrypted sensed data
M	Aggregated data
C	encrypted Aggregated data
A||B	Concatenation A with B
N	Nonce used once to provide the data freshness
MAC(k,m)	Message Authentic Code
E(k,m)	Encryption of m using the key k
D(k,m)	Decryption of m using the key k

3.3 Detailed description of SDTS scheme phases

SDTS scheme consists of four phases, including *initialization*, *key generation*, *data encryption* and *data decryption*, as shown in figure 2. The details is described as follows:

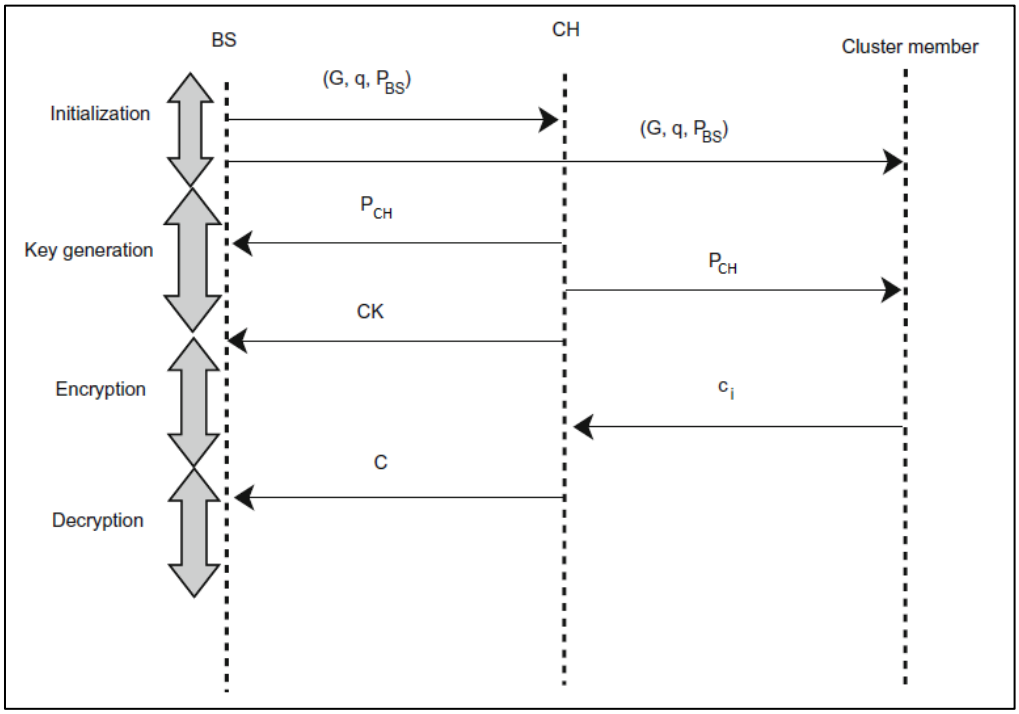

FIGURE 21 ***SDTS'S PHASES****[5]*

3.3.1 Initialization phase

After the deployment of sensor nodes, the BS generates the system parameters by selecting an elliptic curve E, a base point G of order q. Then it picks a random a random number $S_{BS} \in \mathbb{Z}q$ as ephemeral private key, and computes the ephemeral public key $P_{BS} = S_{BS}*G$. After that, BS broadcasts system parameters (G, q, P_{BS}) to whole network. It is worth noting that q represents a large prime number.

3.3.2 Key generation phase

In SDTS scheme, each CH computes ephemeral private and public keys (SCH, PCH) and a secret key SK which is shared between CH and BS. PCH and SCH are used for data encryption and data decryption, respectively. As well, SK key is used to encrypted data signing process.

Note that CH broadcast PCH to its CMs. The generation of keys process is illustrated in Algorithm 1.

Algorithm 1 Key generation phase

Input : G, q, P_{BS}
Output : P_{CH} , S_{CH} , SK
BEGIN
The CH generates a random integer d $\in \mathbb{Z}_q$
The CH calculates S_{CH} by adding d to its ID
The CH computes SK = S_{CH} * P_{BS}
The CH computes P_{CH} = S_{CH} * G then sends it to the BS and its member nodes
The BS computes SK = S_{BS} * P_{CH}
The CH encrypts S_{CH} with SK (i.e. S_{CH} + SK = CK) then sends CK to the BS
The BS decrypts S_{CH} using SK (i.e. CK - SK)
The BS stores the clusters key pair and shared key in a database
END

3.3.3 Data encryption phase

During this phase, each CM encrypts its sensed data using the public key PCH and then sends the result to its CH. The latter aggregates the received encrypted data from its CMs, creates a signature Si for each received data using the key SK. Then, the CH forwards the result to the BS. The data encryption phase is illustrated in Algorithm 2.

Algorithm 2 Encryption phase

Input : m_i, P_{CH} , SK
Output : c_i, C
BEGIN
for each member node i **do**
Select a random number $K_i \in \mathbb{Z}_q$
Compute $V_i = m_i + K_i * P_{CH}$
Send $c_i = V_i||K_i$ to CH
end for{upon receiving c_i}
for each c_i **do**
Create a signature $S_i = V_i + SK$
Appends S_i to c_i
end for
The CH sends C = $V_1||K_1||S_1, V_2||K_2||S_2, ..., V_n||K_n||S_n$ to the BS
END

3.3.4 Data decryption phase

Upon receiving encrypted data, the BS checks the S_{CH} and SK keys on its database in order to verify and decrypt the received encrypted data. The data decryption phase is illustrated in Algorithm 3.

Algorithm 3 Decryption phase

Input : C, S_{CH}, SK
Output : m_i
BEGIN
for each $V_i||K_i||S_i$ **do**
  Calculate S_i - SK
  if S_i - SK $= V_i$ **then**
    Compute $m_i = V_i$ - $K_i S_{CH}$ * G
  else
    Discard the message
  end if
end for
END

3.4 Security weakness of SDTS scheme

In this section we introduce several of the SDTS scheme's security vulnerabilities.

- In SDTS scheme, an adversary can eavesdrop on the distribution of ephemeral public keys of CMs on public channels. Therefore, it can decrypt the sensed data of CMs.
- An adversary can intercept the ephemeral public key of CH and BS, which make them subject to Man-in-the-Middle-Attack.
- In SDTS scheme, an adversary can impersonate a legitimate CH by sending a CH's acknowledgement message. Therefore, cluster members (CMs) within its range can transmit data to the malicious CH, because SDTS clearly does not achieve mutual authentication between CM and CH.
- All messages are exchanged without nonce. An adversary can eavesdrop on the sent data and replay them several times.

3.5 Our proposed security scheme

In this paper, we propose an enhancement of SDTS scheme which aim at securing data communication in cluster-based WSN using elliptic curve cryptography. Our scheme is based on Elliptic Curve Menezes-Qu-Vanstone Scheme (ECMQV) scheme[29] (described in chapter 2) to help cluster members to compute shared secret key SK with cluster head. SKis used for symmetric key operations such as the encryption the mutual authentication. Our choice of ECMQV is due to the fact that this scheme is an authenticated version of the elliptic curve Diffie-Hellman key

exchange.Moreover, we use another cryptographic key to secure the communication between CH and BS, which called Global Key (GK). In order to enhance security, GK is renewed for each round.

The aims of our scheme is:

- Improvement in securityaspect. This is by avoiding security vulnerabilities of SDTS scheme.
- Adding the mutual authentication between CH and its CMs. This propriety is not achieved by SDTS scheme.
- Secure the communications between BS and CH, as well as the communications between CH and CM.
- Enhancing in performance results comparing with SDTS, in terms of computational cost, communication cost and energy consumption.

3.5.1 Network Description

In this work, we consider that the network studied is acluster-based WSN. Here the sensor nodes are resource-constrained devicesand homogeneous in functionalities and capabilities.

However,BS is always assumed trustworthy, reliable and is in chargeconfiguring the nodes before the deployment of network.Moreover, all sensor nodes are distributed randomly. In thiswork, we assume that an attacker is active or passive. BS andall nodes are fixed.x

The sensor nodes report gathereddata to the BS via multi-hop communication where the sensor nodes participate in the routing process. Therefore, in order to minimize the traffic transmission

load and reduce the total energy consumption of the sensor network, each CH collects data from all its CMs, aggregates them and transmits the result directly to BS.

3.5.2 Detailed description of our scheme phases

In this section, we present our proposed secure scheme. It is composed of threephases: *initialization phase*, *shared secret key establishment phase*and *secure data transmission phase*. The detail is described as follows:

3.5.2.1 Initialization phase

Initialization phase is ensured by the BS before network deployment. During this phase:

- The BS generates ECC long-term private and public keys (d_i, Q_i) for each sensor node in the network, then it generates its ECC long-term private and public keys (d_{BS}, Q_{BS}).
- Each node *i* is pre-loaded by ECC long-term key pair (d_i, Q_i).

3.5.2.2 Shared secret keyestablishmentphase

This phase consists twosub phases:keys establishment CM-CH, keys establishment BS-CH

- ✓ **keys establishment CM-CH**

In this phase, both CH and CM generate an ephemeral session key pair (Pi, Si) by randomly generating Si and calculating Pi = Si*G where Si is an integer and G is a generator point on the elliptic curve. Then, theyshare the permanent and ephemeral public keys between them to generate implicit signature Sa to calculatesymmetric key SK. The detail is described in Algorithm 1.

Algorithm 1 - keys establishment CM-CH

BEGIN
CH generates random value as ephemeral secret key S_{CH}.
CH calculates $P_{CH}=S_{CH}*G$.
CH sends (P_{CH},Q_{CH}) to CM
CH generates Sa= (Si+$\underline{x}$ Di) mod n
CH calculate SK=hSa(Pi+$\underline{y}$ Qi)
CM performs a similar computation.
END

- ✓ **Keys establishment BS-CH**

  Each CM deletes the GK and the CH generate di as symmetric key between CHi and BS using GK and delete this last one.

Algorithm 2 - keys establishment BS-CH

BEGIN
CM Delete GK
CH Generate a random value as secret key L_{CH}
CH calculate $C_{CH}=E(GK , L_{CH})$ and $V_{CH}= MAC(GK ,C_{CH},N_{CH})$
CH sends$C_{CH}||N_{CH}$ ||V to BS
CH delete GK
BS calculates$V_{CH}'=MAC(GK, C_{CH}, N_{CH})$
If ($V_{CH}'=V_{CH}$) then BS decrypts C_{CH} using GK to get L_{CH}
And save L_{CH} as shared key between CH and BS
END

3.5.2.3 Secure data transmission phase

Each cluster member CM encrypts the sensed data using SK (shared symmetric secret key with CH). Then, it transmits the result toits CH. After collecting data from all CMs, the CH aggregates these data then forwards the encrypted version to BS.

Algorithm 3 - Secure data transmission

BEGIN

CM encrypts data c_{CM}=E (SK, m_{CM}).

CM computes V_{CM}=MAC (SK, c_{CM},N_{CM}).

CM sends $c_{CM}||N_{CM}||V_{CM}$ to CH.

CH calculate V_{CH}'= MAC (SK, c_{CM}, N_{CM}).

IF (V_{CM}'=V_{CM}) THEN m_{CM}=D (SK, c_{CM}).

CH calculate M_{CH}= agg(m_1,…,mi)

CH calculate C_{CH}=E(L_{CH}, M_{CH})

CH calculate V_{CH} =MAC(L_{CH}, C_{CH}, N_{CH})

CH sends $C_{CH}||N_{CH}||V_{CH}$

BS calculate V_{CH}'=MAC ($L_{CH,}$ C_{CH},N_{CH})

IF (V_{CH}'=V_{CH}) THEN calculates M_{CH}=D(L_{CH}, C_{CH})

END

After sending the data messages, the BS creates a new GK, then encrypts it using L_{CH}. The result is sent to the CH. The latter decrypts the new GK, then it encrypts it using the key SK beforebeing sent to CM.

3.6 Security analysis

Regarding the security aspect, our proposed scheme has the abilityto provide protection for cluster-based WSN by preventing various attacks.

Confidentiality: as we use ECC to encrypt the sensed data in the networks, an attacker cannot figure out or steal the data without decryption key. Moreover, even if the attacker successfully cracks the secret key between CMi and CH he cannot decrypt data between other CMs and CH or get secret key between CHi and BS in one round. Therefore, message confidentiality is ensured and data privacy is well protected.

Mutual authentication:DTS scheme can guarantee authentication between CH and BS by signed with the secret shared key but can't guarantee authentication between CM and CH. Unlike us, we've guaranteed the authentication by based on ECMQV that it uses implicit

signatures to ensure that the data contributed by the parties is authentic and complete in the whole network.

Man in the middle attack resistance:because the performance of ECMQV which this allows protocols that use ECMQV for key agreement to offer stronger authentication and ensure that malicious entities cannot masquerade as a third party to the entity whose key was compromised

Integrity:since each CM signs the sensed or the received data with the secret shared key, the BS and CH can check that the data have not been altered or modified by verifying the signature of the message.

Resilience to replay attack: as the SDTS scheme, all transmitted messagesinclude a random number N that disables the adversary to perform areplay attack.

3.7 Performance analysis

In this section we evaluate the performance of our proposed scheme in terms of computational cost, communication cost and energy consumption.

3.7.1 Computational cost :

We focus only on computation overhead on CH and CM nodes, because the BS is considered a powerful device. Moreover, we exclude the public and private keys computation.The different operations cryptographic used in our scheme and SDTS, as well as their computation times, are listed in Table 6. It worth noting that the computation times are obtained based on WiSMote platform.

TABLE 7EXECUTION TIME OF CRYPTOGRAPIC PRIMITIVES ON WISMOTE

Operation	Notation	Computation time (second)
Shared secret key establishment	ECDH	2.61
Authenticated shared secret key establishment	ECMQV	3.64
ECC-based encryption	E_{ECC}	3.88
ECC-based decryption	D_{ECC}	2.62

AES-128 encryption	E_S	0.004
AES-128 decryption	D_S	0.004
MAC generation / verification	MAC	0.014

On CM side:

1. Establishes the authenticated shared key (SK) with the CH.
2. Encrypts the sensed data using SK.
3. Generates the MAC value using SK.

Thus, the time required for the CM is$ECMQV+E_S+MAC = 3.64+0.004+0.014 =$**3.654** s.

On CH side:

4. Establishes the authenticated shared key (SK) with the CM.
5. Decrypts the sensed data using SK.
6. Verifies the MAC value using SK.
7. Encrypts L_{CH} using GK
8. Generates the MAC value using GK.
9. Encrypts the aggregated data using L_{CH}.
10. Generates the MAC value using L_{CH}.

Thus, the time required for the CH is $ECMQV+2S_E+S_D+3MAC = 3.64+0.008+0.004+0.042 =$**3.694** s.

3.7.2 Communication cost

To calculate the communication cost of our proposed scheme, we defined the following assumptions:

- Public key size is 40 bytes.
- ECC-based encrypted data size is 36 bytes.
- Symmetric-based encrypted data is 16 bytes.
- MAC size is 16 bytes.

- Cryptographic nonce N is 1 byte.
- Number of CMs in each cluster is 10.

The communication of our proposed is divided intotwo phases: Shared secret key establishment and secure data transmission. Where in the first phase is exchanged three messages,two of thembetween CH-CM to generate SK and the last message is between CH-BS to generate di. As for the second phase, it contains two messages one between CM and CH, and the second between CH and BS, in order to send sensed data from CMs to BS through CHs

TABLE 8 COMMUNICATION COST TABLE

Our scheme phases	Nbr of messages	Nbr of bytes
Shared secret key establishment	3	80+80+33=193
Secure data transmission	2	33+33=66

3.7.3 Energy consumption

To estimate the energy consumption on WiSMote platform, we use the equation W = V * I * t, where W, V, I and t are the power consumption in (mJ), the voltage in (V), the current draw in CPU active mode in (mA) and the computational time in second, respectively. It worth noting that the current draw on WiSMote is 2.2 mA and the voltage is 3.0 V.

In our scheme, the computation time required by CM is t = 3.654. Thus, W = 3*2.2*3.654 = 24.116 mJ. While the computation time required by CH is t = 3.694. Thus, W = 3*2.2*3.694 = 24.380mJ.

3.8 Comparative Analysis

This section provides a comparative analysis of our proposed scheme to the SDTS scheme**.** The comparison of security properties and performance is presented in Table

TABLE 9 COMPARATIVE TABLE

Scheme	Security					Performance					
						Computation (sec)		Communication (byte)		Energy (mJ)	
	I	C	A	R	M	CM	CH	K-E	S-D-T	CM	CH
SDTS	-	+	P/A	-	-	3.881	2.745	96	680	25.614	18.176
								Total : 776			
Our scheme	+	+	+	+	+	3.654	3.694	193	66	24.116	24.380
								Total : 259			

The notations used in this comparative table are listed in as follow:

TABLE 10 NOTATIONS

Notation	*Description*
+	Applicable
-	Not applicable
P/A	Partial applicable
I	Integrity
C	Confidentiality
A	Authentication
R	Replay attack resistance
M	Man in middle attack resistance

GENERAL CONCLUSION AND FUTURE WORK

Wireless sensor networks have become an essential component in IoT because they have a particular interest in military applications, environmental, domestic, medical...etc. With this increased dependence on WSN and its association with the Internet, stronger security primitives are necessary to ensure the correct behavior of the sensor nodes on its network.

In this work, we are interested in the security problems in the WSNs, for that SDTS algorithm based on elliptical curves has been analyzed, and emphasize the weaknesses of these Scheme and propose a scheme to improve it based on Elliptic Curve Cryptography which we used with Contiki. and the cryptographic libraries that implement them, and we have chosen the Relic Tool Kit library to be used in the sensors and to evaluate computation cost, the communication cost, and the energy cost by each node in one round. This proposed is considered to be a secure version of the SDTS.

We conclude that our proposed scheme increases the level of security for the SDTS scheme by ensuring the security requirements: Authentication, Confidentiality, Integrity, and the freshness. Thus, it makes it possible to enhance durability against attacks (man in the middle attack, replay attack) against the SDTS scheme. It is also better in terms of communication cost.

For future work, wepropose to researchers in this domain,trying to minimize thecommunication cost in the CH level.

GENERAL CONCLUSION AND FUTURE WORK

Bibliography

1. Atzori, L., A. Iera, and G. Morabito, *The internet of things: A survey.* Computer networks, 2010. **54**(15): p. 2787-2805.
2. Zanjireh, M.M. and H. Larijani. *A survey on centralised and distributed clustering routing algorithms for WSNs*. in *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*. 2015. IEEE.
3. Azzabi, T., H. Farhat, and N. Sahli. *A survey on wireless sensor networks security issues and military specificities*. in *2017 International Conference on Advanced Systems and Electric Technologies (IC_ASET)*. 2017. IEEE.
4. Yun, D.Y., K.-D. Jung, and J.-Y. Lee, *The Routing Algorithm for Wireless Sensor Networks with Random Mobile Nodes.* International Journal of Internet, Broadcasting and Communication, 2017. **9**(4): p. 38-43.
5. Harbi, Y., et al. *Secure data transmission scheme based on elliptic curve cryptography for internet of things*. in *International Symposium on Modelling and Implementation of Complex Systems*. 2018. Springer.
6. Rayes, A. and S. Salam, *Internet of things from hype to reality.* The Road to Digitization; River Publisher Series in Communications; Springer: Basel, Switzerland, 2017. **49**.
7. Jaladi, A.R., et al., *Environmental monitoring using wireless sensor networks (WSN) based on IOT.* Int. Res. J. Eng. Technol, 2017. **4**(1): p. 1371-1378.
8. Zheng, J. and A. Jamalipour, *Wireless sensor networks: a networking perspective*. 2009: John Wiley & Sons.
9. SAHRAOUI, S., *Mécanismes de sécurité pour l'intégration des RCSFs dans l'IoT (Internet of Things)*. 2017, Université Mustapha Ben Boulaid Batna 2, Département de l'informatique.
10. Singh, S.K., M. Singh, and D.K. Singh, *Routing protocols in wireless sensor networks–A survey.*International Journal of Computer Science & Engineering Survey (IJCSES), 2010. **1**(2): p. 63-83.
11. Cazorla, M., K. Marquet, and M. Minier. *Survey and benchmark of lightweight block ciphers for wireless sensor networks*. in *2013 international conference on security and cryptography (SECRYPT)*. 2013. IEEE.
12. Kovatsch, M., S. Duquennoy, and A. Dunkels. *A low-power CoAP for Contiki*. in *2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems*. 2011. IEEE.
13. Roussel, K., Y.-Q. Song, and O. Zendra. *Using Cooja for WSN simulations: some new uses and limits*. 2016.
14. Panda, M., *Security in wireless sensor networks using cryptographic techniques.* American Journal of Engineering Research (AJER), 2014. **3**(01): p. 50-56.
15. Kellner, A., O. Alfandi, and D. Hogrefe, *A survey on measures for secure routing in wireless sensor networks.* International Journal of Sensor Networks and Data Communications, 2012. **1**(10): p. 1-17.
16. Djenouri, D., L. Khelladi, and N. Badache. *Security issues of mobile ad hoc and sensor networks*. in *IEEE Communications Surveys Tutorials*. 2005. IEEE Communications Society.
17. Zhu, J., Y. Zou, and B. Zheng, *Physical-layer security and reliability challenges for industrial wireless sensor networks.* IEEE access, 2017. **5**: p. 5313-5320.

18. Udgata, S.K., A. Mubeen, and S.L. Sabat. *Wireless sensor network security model using zero knowledge protocol*. in *2011 IEEE international conference on communications (ICC)*. 2011. IEEE.
19. Kavitha, T. and D. Sridharan, *Security vulnerabilities in wireless sensor networks: A survey.* Journal of information Assurance and Security, 2010. **5**(1): p. 31-44.
20. Faye, Y., I. Niang, and H. Guyennet. *A user authentication-based probabilistic risk approach for Wireless Sensor Networks*. in *2012 International Conference on Selected Topics in Mobile and Wireless Networking*. 2012. IEEE.
21. Shou, Y., *Cryptographie sur les courbes elliptiques et tolérance aux pannes dans les réseaux de capteurs*. 2014, Besançon.
22. Hsieh, W.-B. and J.-S. Leu, *A robust user authentication scheme using dynamic identity in wireless sensor networks.* Wireless personal communications, 2014. **77**(2): p. 979-989.
23. Mahto, D., D.A. Khan, and D.K. Yadav. *Security analysis of elliptic curve cryptography and RSA*. in *Proceedings of the world congress on engineering*. 2016.
24. Kaur, P. and S. Kalra, *On Security Analysis of Recent Password Authentication and Key Agreement Schemes Based on Elliptic Curve Cryptography.* Journal of Technology Management for Growing Economies, 2015. **6**(1): p. 39-52.
25. ANSI, X., *63: Elliptic curve key agreement and key transport protocols.* Working Draft, Oct, 1998.
26. Lattin, W., *Efficient and authenticated key agreement.*
27. ; Available from: https://code.google.com/archive/p/relic-toolkit/.
28. Kumar, U., T. Borgohain, and S. Sanyal, *Comparative analysis of cryptography library in iot.* arXiv preprint arXiv:1504.04306, 2015.
29. Law, L., et al., *An efficient protocol for authenticated key agreement.* Designs, Codes and Cryptography, 2003. **28**(2): p. 119-134.