Computer Security Symposium 2013
21 - 23 October 2013

# センサネットワークにおける

# 認証子を用いたネットワーク構成確認方式の提案

金子 良† 岩村 恵市†

†東京理科大学大学院工学研究科電気工学専攻
125-8585 東京都葛飾区新宿 6-3-1
kaneko_r@sec.ee.kagu.tus.ac.jp

**あらまし** ワイヤレスセンサネットワークのセキュリティについてのプロトコルには，ノードがネットワーク構成を把握していることを前提としたプロトコルが多数存在する．しかし，ネットワーク構成の安全な確認方式について検討しているものは少ない．CSS2011では，佐藤等によって繰り返し暗号化メッセージを用いた方式が提案されているが，通信回数が増加してしまうという問題があった．本稿では，既存のルーティングプロトコルであるOLSRに認証子を付加することで，通信回数を追加せず，正当なネットワーク構成であるか確認する方式を提案する．

# A method to verify configurations using an authenticator in the wireless sensor network

Ryo Kaneko† Keiichi Iwamura†

†Tokyo University of Science.
6-3-1, Nijuku, Katushika, Tokyo, 125-8585, JAPAN
kaneko_r@sec.ee.kagu.tus.ac.jp

**Abstract** The wireless sensor network security protocol assumes that a node has to identify various network configurations. However, the safety check method considered for network configuration is inadequate. In CSS2011, Sato proposed a method for verifying wireless sensor networks using repeated encrypted messages; however, this method increases the number of transmissions in the network. In this paper, we propose a method for checking authenticated network configurations by using an authentication code with the OLSR protocol, which is an existing routing protocol.

## 1 はじめに

ワイヤレスセンサネットワーク[1]は防災，防犯，軍事などの幅広い分野で活躍が期待されているアドホックネットワークの一種である．ワイヤレスセンサネットワークは，センサノードと呼ばれるセンシング機能を持つ小型端末とベースステーションと呼ばれるセンサノードを管理

する計算機によって構成される．センサノードを多数配置し，配置されたそれぞれのノードがセンシングしたデータを無線通信によってベースステーションに伝達することで情報収集などを行う．ワイヤレスセンサネットワークに使用されるセンサノードは主に電池駆動することが想定され，電力の補充が考えられていない．そのため，低電力化が重要視されている．また，センサノードは限られた演算能力しか持たないため，公開鍵暗号など複雑な計算を行うことが難しい．さらに，センサノードは物理的に安全でない場所に設置されることが多く，耐タンパ性を持たない．よって，攻撃者はノードを盗難して暗号化に関する情報を解析することは容易である．センサノードに対して，ベースステーションはネットワーク全体の管理を行う計算機であり，センサノードでセンシングされた情報はベースステーションに集められるため，ベースステーションは耐タンパ性を持ち，安全な場所で管理される場合が多い．また，ベースステーションは収集された大量の情報を処理する必要があり，演算能力は高く，電源容量に制限はない場合が多い．

今までのワイヤレスセンサネットワークのセキュリティに関する研究では，ノードがネットワーク構成を把握していることを前提とするプロトコルが存在する[2][3]．ネットワーク構成を把握するためには，定められたルーティングプロトコルによって，ネットワークを構成するための制御情報をノード同士が自律的にやりとりすることでネットワークの構築が行われる．しかし，このネットワーク構築またはネットワーク構成把握は通信プロトコルに関する部分であり，セキュリティについて検討された提案は少ない．CSS2011 では，佐藤等によって繰り返し暗号化メッセージを用いたネットワーク構成確認方式[4]が提案されている．佐藤等の方式は，ベースステーションが把握したネットワーク構成を確認するために，ルーティング順序に従って繰り返し暗号化されたメッセージを生成し，各ルートごとに送信する．このメッセージは，ネットワーク構成が正しい場合のみにエンドノードで復号することができ，復号結果から生成した受信確認をベースステーションが検証することでルート情報が正しいか確認することができる．これによって，攻撃者が不正なルート情報をベースステーションに申告した場合，そのルートは使われないため，センサノードの不正な利用を防ぐことができる．

しかし，低電力化が重要視されるワイヤレスセンサネットワークでは，通信回数を少なく抑えることが望ましいが，佐藤等の方式ではルーティングプロトコルの制御メッセージとは別にルート情報を検証するためのメッセージを送信しなければならず，通信回数が増加してしまうという問題点があった．そこで，本稿では既存のルーティングプロトコルであるOLSR[5]の制御メッセージにネットワーク構成確認のための認証子を付加することで，通信回数を抑え，正しいネットワーク構成であるかを確認する方式を提案する．

本稿では，第 2 章で既存のルーティングプロトコルについて説明し，第 3 章でネットワーク構成の攻撃について説明する．第 4 章では，従来方式である佐藤等の方式を説明し，第 5 章で既存のルーティングプロトコルである OLSR に認証子を付加した方式を提案する．6 章で従来方式と提案方式に関して考察を行う．

## 2　ルーティングプロトコル

本章では，センサネットワークに適用可能と考えられるアドホックネットワークのルーティングプロトコルに関する分類と本提案方式で用いる OLSR の説明する．

### 2.1　ルーティングプロトコルの分類

アドホックネットワークにおいては各ノードが無線通信範囲外のノードと通信する場合には，中間のノードが中継をする．この中継機能を持たせるためにアドホックネットワーク特有のルーティングプロトコルが必要である．これまでに，

提案されてきたプロトコルの分類を以下に示す.

表 1 ルーティングプロトコルの分類

| 分類 | プロトコル例 |
|---|---|
| プロアクティブ型 | OLSR, TBRPF |
| リアクティブ型 | DSR, AODV |

2.1.1 プロアクティブ型

プロアクティブ型ルーティングプロトコルは送信要求が発生する前に互いのノードが通信しあい，あらかじめ各ノードへの経路表を保持しておく. そのため，通信要求が発生した場合に即時にデータを送信することができる. また，定期的に経路表の更新を行うことで，新たなノードがネットワーク内に入ってきた場合やネットワークから切断されたノードに対応することができる. しかし，定期的に経路表を更新するためにデータを通信しない際にも制御情報流す必要があり，消費電力が大きくなってしまう. プロアクティブ型ルーティングプロトコルはノードがあまり移動しないネットワークに適している.

2.1.2 リアクティブ型

リアクティブ型ルーティングプロトコルは送信要求が発生した際に，経路表を構築する. そのため，データの送信までに遅延が生じてしまうが，データを通信しない際に制御情報を流す必要がないため，消費電力を抑えることができる. リアクティブ型ルーティングプロトコルはノードの移動が頻繁なネットワークに適している.

## 2.2 OLSR

OLSR(Optimized Link State Routing)はRFC3626で提案されているプロアクティブ型のルーティングプロトコルである. センサネットワークはノードの移動が少ないと考えられるので，プロアクティブ型が適していると考えられる. プロアクティブ型の基本的な特徴は 2.1.1 節で示したが，OLSR の大きな特徴として，フラッディングを効率化するために MPR(Multi Point Relay)集合を用いていることである. フラッディングとは，宛先不明のノードへメッセージを送信を行ったり，ネットワーク中のすべてのノードへメッセージを送信したりする手段である. 以下に，OLSR の概要を示す.

2.2.1 MPR 集合

MPR集合とは，メッセージのフラッディングを行う際に，再送信を行うノードの集まりである. この再送信を行うノードは各ノードごとに予め選択されている. また，あるノードが MPR として選択しているノードをそのノードの MPR セレクタ集合と呼ぶ. この情報を管理することで，各ノードはどのノードから受信したメッセージを再送信すればよいかを把握することができる.

2.2.2 メッセージ

OLSR のメッセージには 4 種類のメッセージがあるが，本稿ではHELLOメッセージとTCメッセージの 2 種類について説明する.

① HELLO メッセージ

HELLO メッセージは，各ノードが持つ情報の通知を目的として定期的に送信されるメッセージである，HELLO メッセージによって周辺情報の収集を行う. OLSR では，ローカルリンク情報として 5 つの要素を含む情報を管理しており，HELLO メッセージをやり取りすることでローカルリンク情報を構築する. 以下に，ローカルリンク情報の要素とHELLOメッセージのフォーマットを示す.

●リンク集合
直接的に電波が届くノードの集合

●隣接ノード集合
各隣接ノードのアドレスやそのノードへの再送信の積極度により構成される集合

●2ホップ先の隣接ノード集合
隣接ノード集合のさらに先に存在するノードの集合とそれらと直接通信できるノードによって構成される集合

●MPR 集合
MPR として選択された隣接ノードの集合

●MPR セレクタ集合

自身の MPR として選択しているノードの集合

② TC(Topology Control)メッセージ

TC メッセージは，ネットワーク全体のトポロジを各ノードに通知するためにフラッディングされるメッセージである．各ノードはそのトポロジ情報を基に経路表を構築する．TC メッセージに含まれる要素を以下に示す．

●自身のアドレス

●近隣広告シーケンス番号

近隣ノードの変化を検知するたびに増加する

●近隣広告アドレス

MPR セレクタ集合を広告アドレスとして格納

TC メッセージは MPR として選択されている全てのノードによって定期的に送信され，TC メッセージには自身と MPR セレクタ集合間の接続情報が含まれている．そのため，ネットワーク上の全てのノードは MPR とその MPR セレクタ集合を知ることができる．以下に各メッセージのフォーマットを示す．


(a)OLSR パケットフォーマット


(b)HELLO メッセージフォーマット


(c)TC メッセージフォーマット

図 1 OLSR の制御メッセージパケットフォーマット

## 3 経路に関する攻撃

ルーティングプロトコルでは，経路表の作成には制御情報のやり取りによって行われる．しかし，これらの情報はセキュリティ情報を含まないため攻撃者は容易に改ざんすることができる．また，ワイヤレスセンサネットワークにおいて全てのノードはベースステーションによって管理されているため，ベースステーションの利用するルート情報はセキュリティ上非常に重要である．

制御情報改ざんの例として OLSR の制御情報を取り上げると，ネットワーク内の攻撃者は，実際には存在しないノードを記して HELLO メッセージや TC メッセージを生成したり，他のノードになり済まして HELLO メッセージや TC メッセージを生成することなどが考えられ，これによってベースステーションに偽のルート情報を認識させるが可能となる．この時，ネットワーク内にネットワーク内に攻撃者ノードがルート情報を改ざんする攻撃の種類として次のものが考えられる．

① ノードが存在しないにもかかわらず，存在すると偽る攻撃

② 実際存在しているノードとは異なるノードに接続していると偽る攻撃

③ ノードが存在しているにもかかわらず，存在していないと偽る攻撃

①，②攻撃が行われた経路情報をベースステーションが使用した時，あるノードに対してメッセージを送りたいにもかかわらず，実際には存在しないノードを経由することになっているため通信を行うことができない．また，③の攻撃を行った場合，攻撃者はベースステーションに知られずに存在していないと偽ったノードを利用することも可能となる．これらの攻撃はワイヤレスセンサネットワークへの攻撃研究[6]においてワームホール攻撃やブラックホール攻撃，シビル攻撃などと呼ばれている．

# 4　従来方式

従来方式として，プロアクティブ型プロトコルによって得られたルート情報が正当なルートであるかどうかを確認する方式として佐藤等の方式がある．本章では，佐藤等の方式について説明する．

## 4.1　前提条件

各ノードは固有鍵を持つ．また，ベースステーションは全てのノードの固有鍵リストを持ち，これを自由に利用することができる．さらに，各ノードはこの確認手法を理解しており，ベースステーションから下記暗号化メッセージが送られてこない時，上位ノードに不正者がいるとみないし，それ以降の通信を行わないとする．

## 4.2　従来方式の動作

本方式では，ベースステーションが各ノードから送られてくる経路作成のための制御メッセージから経路表を作成し，図 3 のようにネットワーク構成を把握したとする．

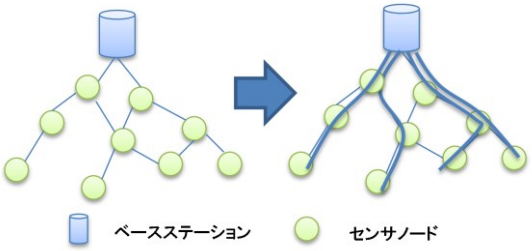


図 2　ベースステーションによるルート選択

この時，ベースステーションは得られたネットワーク構成から図 3 のようにルート情報に従って 1 直線のルートを選択する．

ベースステーションはルート情報を確認するために，繰り返し暗号化を利用したメッセージを作成する．繰り返し暗号化とは 1 つの平文に対して，複数の鍵を使用して繰り返し暗号化を行う暗号方式である．繰り返し暗号化を利用することで，暗号化で使用した鍵を逆順で用いた場合のみ完全な復号化が可能となる．

また，暗号化する平文にハッシュ連鎖の最新値を用いる．ハッシュ連鎖とは，あるランダムな値に対してハッシュ関数を任意回数施したものである．ノード管理者がこのハッシュ連鎖を生成し，事前に連鎖列の最終値を全てのノードと共有しておく．ベースステーションは，すべてのハッシュ値を知っており，まず最終のハッシュ値の1つ前のハッシュ値を送信し，ノードは送られたハッシュ値を再ハッシュ化して，自分が持つ最終のハッシュ値になることを確認する．これによって，そのメッセージの送信者がすべてのハッシュ値を知るベースステーションであることを認証する．ベースステーションとノードはメッセージを送信するたびに，1 つ前のハッシュ値を最終値として更新することにより，その後も送信者がベースステーションであることを認証することができる．

# 5　提案方式

従来方式では，経路情報の正当性を検証するために繰り返し暗号化されたメッセージをルーティングプロトコルの制御メッセージとは別に，各ノードへ送信する必要があった．そのため，各ノードの通信回数が増えてしまい，電源に限りがあるワイヤレスセンサネットワークにおいて好ましくない．そこで，既存のルーティングプロトコルである OLSR の制御メッセージに認証子を付加することで，通信回数を増やさず，経路情報の正当性を検証する方式を提案する．

## 5.1　前提条件

各ノードは固有鍵を持つ．また，ベースステーションは全てのノードの固有鍵リストを持ち，これを自由に利用することができる．さらに，各ノードはブロードキャストメッセージ認証方式である TESLA を利用することができる．ブロードキャストメッセージ認証方式は，通常，公開鍵暗号を基にした技術であるが，TESLA は共通鍵暗号のみを用いており，演算能力に限りがあ

るワイヤレスセンサネットワークに適している.

## 5.2 提案方式の動作

既存のルーティングプロトコルである OLSR では経路表を作成するのに HELLO メッセージと TC メッセージの 2 つを用いる. OLSR では, HELLO メッセージのやり取りによって, ①隣接ノードの探索, ②隣接ノードとのコネクション確立, ③MPR, MPR セレクタ集合の決定が行われる. その後, MPR として選ばれたノードが TC メッセージをネットワーク全体にブロードキャストし, これをもとにルーティングテーブルの作成が行われる. 本方式では, HELLO メッセージのやり取りの後, MPR として選ばれた TC メッセージに認証子を生成し付加する. OLSR では, TC メッセージはフラッディングされるため, ベースステーションも全ての認証子付き TC メッセージを受信することができる, ベースステーションは, 受信した TC メッセージの認証子を検証する. もし, 不正なノードが発見された場合, 不正ノードリストに登録し, ブロードキャストメッセージ認証方式である TESLA を用いて全ノードに伝える.

### 5.2.1 TC メッセージ用認証子生成方法

TC メッセージ用認証子の生成は MPR となったノードが生成する. 図 3 では, MPR に注目した接続関係の例を表している.

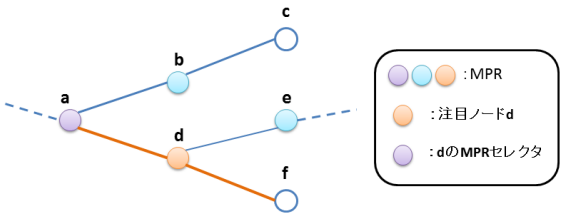


図 3 MPR に注目した接続関係の図

図 3 の a,b,d,e のノードはそれぞれ MPR である. 今回, この中から a,d,e,f のノードに注目して説明する.

TC メッセージに含まれる主な情報は送信元(MPR)アドレスと近隣広告アドレスである. 近隣広告アドレスには, MPR セレクタが含まれ, 直接接続している MPR でないノードが含まれる. 今回の近隣広告アドレスはノード a とノード e とノード f のアドレスが含まれる. MPR であるノード d は以下の手順でノード a, e, f と情報を交換し, 認証子を生成する. 以下に認証子生成の詳細を示す.

① MPR(ノード d)は乱数 $r$を生成し, 近隣広告アドレスのノード(ノード a, e, f)に乱数送信する.

② 近隣広告アドレスのノード(ノード a, e, d)は, $H_a=h(r||K_a), H_e=h(r||K_e), H_f=h(r||K_f)$ のように受信した乱数 $r$と自らの固有鍵の連接のハッシュ値を MPR へ返信する.

③ MPR は $MAC_{Kd}(H_a||H_e||H_f)$のように受信した近隣広告アドレスのノードのハッシュ値の連接を平文とし, MPR の鍵を用いて認証子を生成する.

MPR はこのような手順で生成した認証子 $MAC_{Kd}(H_a||H_e||H_f)$と認証子生成に利用した乱数 $r$を TC メッセージに付加し, 認証子付き TC メッセージとしてネットワーク全体にブロードキャストする. 通常の TC メッセージを拡張したため, 新しいパケットフォーマットが必要となる. 認証子付き TC メッセージのパケットフォーマットを図 4 に示す.

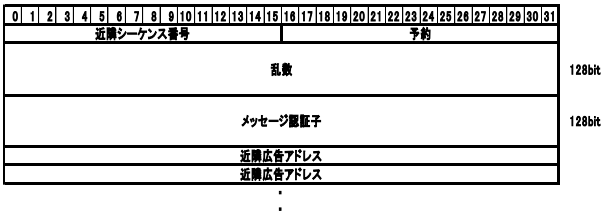


図 4 認証子付き TC メッセージのパケットフォーマット

### 5.2.2 ノードによる認証子の検証

MPR が認証子付き TC メッセージを送信する際, 近隣広告アドレスのノードは MPR が正しく認証子付き TC メッセージを生成しているかどうかを確認する. MPR と近隣広告アドレスのノードは直接接続可能な範囲にあり, MPR が認証子付き TC メッセージを送信した際, 必ず受信

することができる.

近隣広告アドレスのノードのうち，MPR セレクタは HELLO メッセージの交換により MPR がどのノードと直接接続しているかを把握している. MPR に直接接続しているノードは，自らもMPRとして選択されTCメッセージをブロードキャストするか，MPR の TC メッセージに近隣広告アドレスとして記載される. そのため，MPR セレクタは認証子付き TC メッセージを確認し，MPR に直接接続しているノードが，近隣広告アドレスとして含まれているかを確認する. 含まれていないノードに関しては，そのノードから TC メッセージが送られてくるかを確認する. もし，MPR が接続関係を偽っていた場合，偽って追加したノードの固有鍵を持たず，偽って追加したノードを近隣広告アドレスに含めた認証子付き TC メッセージを生成することはできない. また，偽って追加したノードが作る認証子付き TC メッセージを生成することもできない. よって，MPR の接続関係の偽装を検知することができる.

近隣広告アドレスのノードのうち，MPR セレクタ以外のノードは，自らのアドレスが確かに TC メッセージの近隣広告アドレスとして含まれているかを確認する. もし，含まれていない場合，ネットワーク全体に自らのノードの存在を知らされることがなくなり，MPR に自らが不正利用される可能性があるため，メッセージの送受信を停止する.

#### 5.2.3 ベースステーションによる認証子の検証

MPR によって生成された認証子付き TC メッセージは全てベースステーションによって検証される. 認証子生成に使用した情報は乱数 $r$，MPR の鍵，近隣広告アドレスの鍵である. ベースステーションは全ノードの固有鍵リストを持っているため，TC メッセージに含まれるアドレスを参照することにより，認証子生成に使用された鍵を得ることができる. このように，ベースステーションは，送られてきた情報と自らの持つ情報を組み合わせることで，認証子を生成することができる. 自らの持つ情報をもとに生成した認証子と送られてきた認証子を比較検証し，相違があった場合 MPR セレクタを不正ノードとして不正ノードリストに登録する.

この不正ノードリストはブロードキャストメッセージ認証方式である TESLA を用いてネットワーク全体にブロードキャストする. TESLA を用いているため，このメッセージを受信したノードは確かにベースステーションから送られてきたメッセージであり，また，改ざんされていないことを確認することができる. 受信した不正ノードリストを参照し，隣接ノードが含まれていた場合，このノードとのリンクを切断する. もし不正ノードリストがベースステーションから届かなかった場合は，上位に攻撃者がおり，自らが不正利用される可能性があるため，メッセージの送受信を停止する.

## 6 考察

### 6.1 安全性

不正な情報収集や不正なセンサノードの利用を経路情報改ざんによっておこなう方法として，以下の 3 つについて評価を行う.

① ノードが存在しないにもかかわらず，存在すると偽る攻撃
② 実際存在しているノードとは異なるノードに接続していると偽る攻撃
③ ノードが存在しているにもかかわらず，存在していないと偽る攻撃

本提案方式では，接続しているノード全ての秘密情報を用いて，セキュリティ情報を生成する必要がある. そのため，攻撃者が不正に追加したノードの秘密情報を持っておらず，セキュリティ情報を生成することができないため，①，②の攻撃を行うことができない.

③の攻撃方法が行われた場合，存在を偽られたノードは攻撃者に不正に利用される可能性がある. しかし，本提案方式では，存在を偽られたノードは攻撃の有無を検知し，自ら動作を停止するため，攻撃者に不正に利用されるのを

防ぐことができる.

### 6.2　通信回数の比較

追加される通信回数は提案方式が優れている. 提案方式では, 認証子付きTCメッセージの生成に関して MPR から近隣広告アドレスに含まれるノードへの乱数の送信に 1 回, 認証子の送信に 1 回である. 認証子の送信は TC メッセージと同時に行われるため, 追加の通信が行われない. ベースステーションが認証子を検証した後, 不正ノードリストをブロードキャストする必要があり, 追加される通信はこの 1 回のみである. よって, 計3回の通信が追加される. 一方, 佐藤等の方式では, 1 つのルートに対してベースステーションが生成した暗号化メッセージの転送に 1 回, この復号結果をもとに各ノードが生成する受信確認の転送が 1 回の通信が行われる. つまり, m 個のノードでは2m回の通信回数である. また, ベースステーションによる受信確認の検証結果のブロードキャストに 1 回の計 1+2m 回の通信が追加される.

### 6.3　計算量の比較

計算量を提案方式と佐藤等の方式で比較すると提案方式の方が優れている. 特に, ベースステーションの計算量に差が大きく生じる. 提案方式ではベースステーションが認証子を検証するが, この認証子は MPR の数と同数であり, ネットワーク全体のノード数よりも少なくなる. 一方, 佐藤等の方式で生成する繰り返し暗号文は, 経路上の全てのノードの固有鍵で暗号化する. ベースステーションの選択するルートによっては, 複数回同じノードを通ることもあり, ネットワーク内の全ノード数以上の暗号化回数が必要となる. また, 佐藤等の方式では, 各ノードが繰り返し暗号の暗号化と復号を行う必要があり, 多くの計算量がかかってしまう.

## 7　まとめ

本稿では, 既存のルーティングプロトコルである OLSR の TC メッセージに認証子を付加することで, 経路情報が正しいかどうかを確認する方式を提案した. また, 本提案方式は, 佐藤等の方式と比べ, 通信回数を抑えることができ, ワイヤレスセンサネットワークに適している.

今後の課題としては, TC メッセージの生成を行うノード以外からの攻撃について詳細を詰める必要があること, 具体的なオーバヘッドの検証を行う必要があることがあげられる.

## 謝辞

本研究を行うにあたり, 多くのアドバイスを頂きました佐藤晃司様に感謝いたします.

## 参考文献

[1] ユビキタスセンサーネットワーク技術に関する調査研究会
http://warp.ndl.go.jp/info:ndljp/pid/235321/www.soumu.go.jp/s-news/2004/040806_4_b2.html
[2] 八百 健嗣, 松村 靖子, 福永 茂”センサネットワークにおける高信頼ブロードキャストメッセージ認証方式”, CSEC,2005, 241-246
[3]酒見 由美, 伊豆 哲也, “センサネットワークにおける効率的な事前共有鍵の配布方法,” SCIS2013, 2F1-3, 2013.
[4] 佐藤 晃司, 岩村 惠市, “センサネットワークにおけるネットワーク構成確認方式の提案とブロードキャストメッセージ認証への応用”, 2011 年 コンピュータセキュリティシンポジウム (CSS2011), 2B4-3, October 2011.
[5] T.Clausen, Ed.:”Optimized Link State Routing Protocol(OLSR)”, RFC3626(2003).
[6] 2010 13th International Conference on Network-Based Information Systems, Wireless Sensor Network Attacks and Security, Mechanisms : A Short Survey, David Martins and Hervé Guyennet, Computer Science Department, University of Franche-Comté, France