ANALYSIS AND ELIMINATION OF ATTACKERS IN WSN USING SECURE MULTIPATH ROUTING PROTOCOL

S.M.Udhayasankar[1] , V.Vijaya Chamundeeswari[2] and Jeevaa Katiravan[3]
[1,2,3]Department of CSE,Velammal Engineering College, Chennai

Abstract : *Wireless Sensor networks are usually marshalled as group of nodes with a communication infrastructure leading to new structure of WSN called Cluster or Hierarchial WSN.In WSN, a primary requirement for the establishment of communication among nodes is that nodes should collaborate with each other. In the presence of malicious nodes,if the nodes interact or collaborate with each other,this will result in serious security issues; for example, such nodes may destroy the routing process. In this scenario, avoiding or diagnosing malevolent nodes launching DOS attacks through shortest path is a challenge.In existing system,to avoid and detect the malevolent cluster member and head,learning based energy prediction algorithm is used whose limitation is node failure,lack of direct communication,excess of energy consumption.This paper attempts to resolve this issue by designing a Secure Multi path Dynamic Routing Protocol based routing mechanism, which is referred to as the Attack Prevention Trust Scheme , that consolidates the advantages of both intense and sensitive defence architectures.*

Keywords : *DOS,Multipath dynamic routing,shortest path,Cluster node*

1. Introduction

A wireless sensor network is a group of nodes formulated into a combined network A wireless sensor network (WSN) has critical purposes such as monitoring remote locations and to keep track of targets.These sensors are provided with wireless interfaces with which they can interact with one another to construct a network.The latest technology in distributed computing have set up in the past few years the emergence of a different wireless sensor network applicationswhich includes military , disaster management, health, industry, and other domains.

For substantial application such as smart cities,security and emergency,e-health,logistics,domestic and home automation ,wireless sensor networks (WSNs) are deployed in a several areas, with a more number of sensor nodes detecting and reporting some information of urgencies to the end-users.Since there cannot be a communication infrastructure, people are likely to use Wireless sensor devices to impart and transfer data between sensor nodes. When an unfavourable event occurs(example.,leakage of gas or breakout of fire),the sensors are used to monitor these events are detected and an alarm is raised to alert the remaining nodes. On getting the aid of programs,feedback for each event

occured is set and the required measures can be taken by the end-users.

The latest advancement in computing and embedded systems have given rise to distinct wireless sensor network applications such as education,security,e-health and military operations.Wireless sensor network comprises of sensor nodes powered by sensing the data,computing and communicating the response to the end users.These nodes have limited power and resources.The batteries used by the nodes are expensive.Hence it is difficult to replace them or overuse them.Geographic location of the node plays an important role in sensing arena.As sensor nodes for tracking the events are established toperform for a long time without frequently charging their batteries, sleep scheduling method is normally employed during the process.

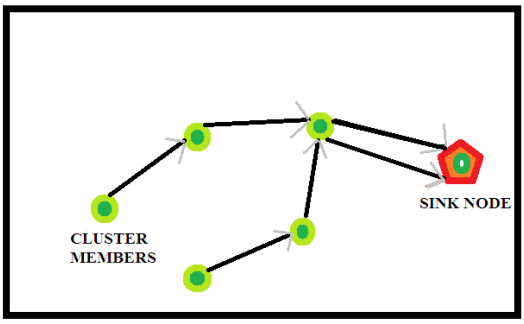


FIGURE 1: Communication between cluster members and sink node

1.1 DoS Attack A denial-of-service (DoS) attack happens when several systems flood the targeted system or the web servers.This attack is said to be a result of multiple systems that are targeted ,thence blocking the system with network traffic.It is designed to receive commands and act accordingly without the knowledge of the administrator.The newer connections cannot be created as the network is blocked with unnecessary traffic.These attacks are harder to prevent as it is harder to track and detect.This may result in complete crashing of the system for indefinite time period. DOS attack allows information and sensor node in network to compromise. Denial of Service (DOS) attack is type of attack which targets to mess up the network by damaging resource capability. In general attacker sends worthless messages to increase network traffic apart from this the attacker also reducethe life time of the network and the node.The life of the network is directly proportional to the capacity of the battery in WSN . Therefore when the battery drains fastly it directly reduces the node's lifetime. The proposed solution for this is AODV

routing protocols in WSN.

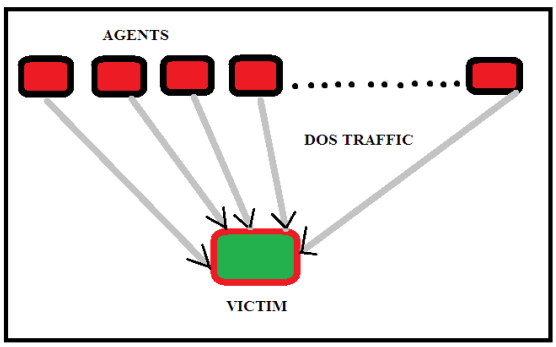


FIGURE 2: Representation of DOS attacks and victims.

1.2 Multipath Routing Multipath routing lessen the importance of security attacks collected from combining malicious nodes in MANET, by increasing the count of nodes that must compromise to take over the control of the information. In this paper, we describe various attacks that Provide multipath routing protocols more sensitive than it is expected.we propose a entire on-demand multipath routing protocol, the Secure Multipath Routing protocol, which gives efficient protection against DoS attacks .

1.3 Ad hoc On Demand Distance Vector (AODV) routing algorithm is a routing protocol meant for ad hoc mobile networks. It constructs routes between nodes in the manner desired by the nodes which acts as source.They maintain these existing routes until they are required by the sources.

2. Related Works

There are several current investigation in identifying and eliminating DoS attacks in WSNs.

[1 & 2] They always have the target on the misdeed of sensor nodes. The available schemes in security provide considerable resources to Supervise the performance of all the sensor nodes. After the detecting the nodes which are corrupted, most schemes build a blacklist to separate malicious nodes. Anyhow, none of them accept the energy character in revealing malvalent nodes . [3] The major focus is to analyze and check out the performance of routing protocols which includes Ad hoc On Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) . It is meant for monitoring of analytical circumstances with the help of certain metrics such as throughput and end-to-end delay in various strategy. [4]This provide a detail on available security attacks in WSNs and the interrelated IDS protocols to outfit those attacks. We investigate the works on regards of network structure of WSNs.apart from this, we emphasize several crucial drawbacks that IDSs right now have and specify future research tasks. [5] Researchers proposed a system known as Spontaneous Watchdogs.

This technique make use of local and global agents to watch over the communications. In hierarchal sensor networks, these global agents are trigerred in each cluster head. Each packet circulating in the network, global agents with the Spontaneous Watchdogs mechanism are able to receive both the packet and the relayed packet by the next-hop. In case of modification of malevolent nodes or particular forwarded packets, then the global agents are capable of detecting the attack . they are done with the help of watch dogs.[6]Grid Routing protocol in WSN is a power **conserving method** for multi-hop ad hoc wireless networks .It lower consumption of energy without reducing the measure of capacity or the network connectivity. It is observed that ,with in a network when there is the presence of nodes with sufficient density in specified region, delegated algorithm is used which allows nodes to make local decisions on whether to sleep, or to join a forwarding as a cluster head. It is showed using the enery model.further , this grid protocol also the enhances capacity of communication.

The objective of this paper is to clarify the issue of detecting and preventing the attacks by implementing a Secure Multi path Dynamic Routing Protocol which is based routing mechanism, which can be called as the scheme of attack prevention, that combines the profit of both dedicated and reactive defence architectures.

Advantages :

- ✓ packet delivery ratio can be improved .
- ✓ Throughput can be enhanced. slightly
- ✓ Reduced average end-to-end delay
- ✓ Routing overhead of messages.

3. Existing System

WSN are arranged as cluster which gives a all new dimension for WSN called cluster or hierarchical WSN where the head of the cluster nodes acts as a sink node(intermediate node) which coordinates the activities of all other nodes in data communication therby transmitting the data that is sensed to gain energy efficiency. The head of the cluster accounts for its cluster and the other nodes in the network. Such a network is vulnerable to attacks like Passive attacks,Active attacks, Cryptographic primitive attacks, DOS attack,Black hole attack etc. The attacks specified tries to act as ordinary node

and enters the network thereby changing the operations of the nodes in the network to destructive operations which may lead to packet drop or change of source or destination nodes in a communication. The malevolent nodes may crowd the network with unnecessary data and irrelevant information. Destructive attacker node fills with unnecessary traffic the and thence taking a toll in bandwidth and energy.The attacking nodes consumes more energy based on various characteristics and the type of destruction it is going to cause.Each attack can be differentiated in terms of the energy that it has consumed and by plotting the energy graph of a network and its nodes. Flooding attack and Gray hole attack have been already studied and implemented as distributed IDS scheme.

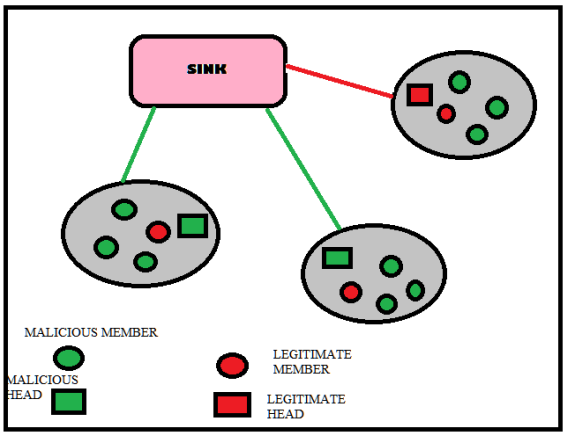


FIGURE 3:Representation of legitimate nodes and malicious nodes

If the energy graph is exact and accurate then thesimulation model designed is said to be accurate else approximation occurs.Weight factor helps in accuracy. Simulations are carried on for flooding attack and gray hole attack in NS2 and each of its characteristics are verified.

4. Proposed system

To enhance the basic model of analyzing the characteristics of the attacks ,this proposed system aims to examine the DOS attack and its characteristics and the energy that it consumes.This paper also inspects the shortest path through which a node can transmit data from an assigned source to destination without the intervention of malicious nodes. Also this paper aims to implement grid arrangement of the nodes i.e., to use resources from multiple locations that are arranged in grid fashion.

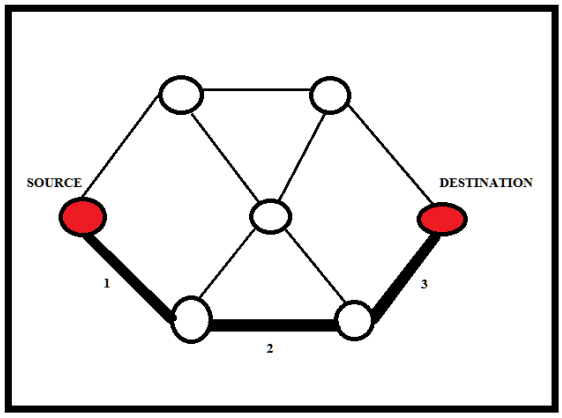


FIGURE 4: Representation of legitimate nodes and malicious nodes

Where the existing system provides prevailing nodes normal communication,the architecture proposed insists on communication between nodes without shortest path.

4.1 Algorithm

- ✓ Let S1,S2……Sn be the sensors nodes that are to be installed.
- ✓ Input and install the sensors S1,S2,S3….Sn.
- ✓ Identify the attackers A1,A2,A3…..An.
- ✓ Install sink base station Sink1,Sink2…Sink n.
- ✓ Source sensor SRC communicates to Base Station BS.
- ✓ Collected Data From Sensor BS is sensed to all neighbors(s2,s3…).The data discovered is updated every few seconds.
- ✓ The information includes Location information and sensor information.
- ✓ Attacker nodes (A1,A2..)enters the network.

Check Energy Level
If (Attackers<==True)
{
Attackers spread infection near nodes
(DOS Attack in shortest path with grid)
BS Destroyed to Attackers
}
Else
Normal Data Collection from Sensors
End if

- ✓ Apply secure multipath dynamic routing protocol
- ✓ Analyze performance based graph results

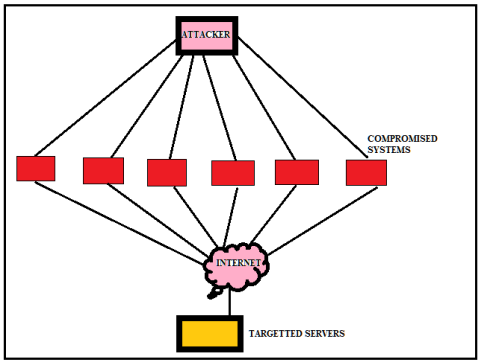


FIGURE 5: Representation of targeted systems and compromised systems.

A wireless channel in a network can be set as follows

set chan [new $val(chan)];

A call to the AODV protocol and SMDRP is made as follows

set val(rp) AODV ;

set val(Agent) SMDRP ;

4.2 AODV AND SMDRP

Usually Mobile adhoc networks(MANETs) are group of mobile nodes with links that are madefor communication purposes. In Multipath Routing Schemes a robust system can be developed.By implementing Secure Multipath Dynamic Routing Protocol (SMDRP) and Adhoc On demand Routing

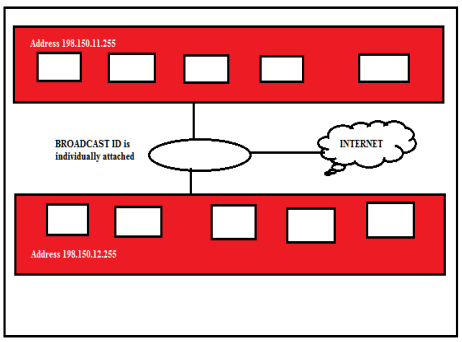
protocol into a group of nodes security factor of the network is taken care off.The purpose of simulation is to evaluate the cost of the present algorithm.

4.3 SECURE MULTIPATH DYNAMIC ROUTING PROTOCOL

Broadcast ID management function

```
Void SSMDRP::id_insert(nsaddr_t id,
u_int32_t bid) {

BroadcastID *b = new BroadcastID(id,
bid);

 assert(b);

b->expire = CURRENT_TIME +
BCAST_ID_SAVE;

LIST_INSERT_HEAD(&bihead, b,
link);

}
```

FIGURE 7: Representation of broadcast management functions .



Initially Link layer detection is performed on the initial nodes.The route is narrowed down and route error upstream is sent.An assert is then evoked followed by inserting Broadcast Id management functions.A lookup is performed a match of source id and destination id is checked.Helper functions are also added.A separate provision is made for link failure management functions(exceptions handling).In case of route failure these set of functions are called.Non data packets and broadcast packets with no data can be dropped. If the broken link is closer to the destination than source, a local repair is attempted. Otherwise, the route is brought down. A route request is sent to forward the packets. The packets are buffered. If the attacker tries to forward a packet for some other node to which it doesn't have a route and authorization then drop the packet and upstream error is sent.If the valid route is expired then all packets are purged from send buffer and the route is invalidated.The time taken to live is also checked.

```
Expiry time = CURRENT_TIME +
ACTIVE_ROUTE_TIMEOUT
```

5.SIMULATION RESULTS:

Any low level attacks and DOS attacks made by the attacker are successfully identified and eliminated using Secure Multipath Routing Protocol.

5.1 **NETWORK DEPLOYMENT:** Network deployment simulation is used to opt for different range of hardware and software configuration according to the need.

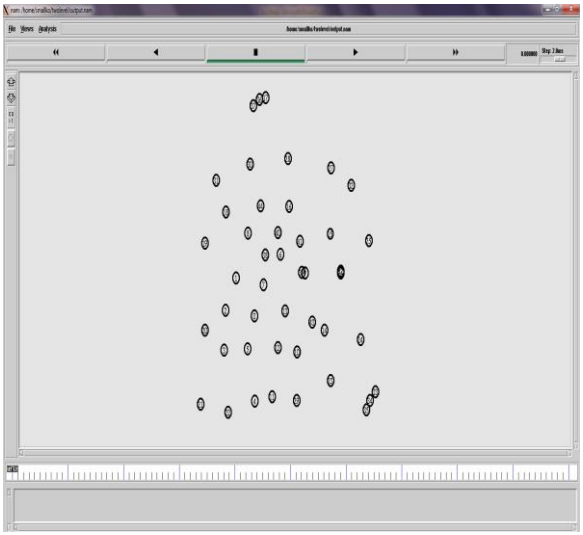


FIGURE 8: Representation of network deployment.

5.2 DATA COMMUNICATION:

This figure shows the data communication between two nodes ad how the sensor node senses the presence of neighbor nodes in a network with large number of nodes.

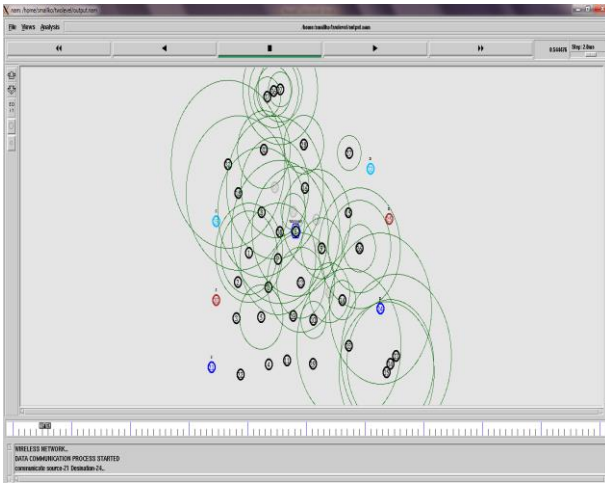


FIGURE 9: Representation of data communication between nodes

5.3 SHORTEST PATH

This figure is the actual start process of the secure multipath dynamic routing protocol wherein shortest path transfer of data from source to destination occurs.

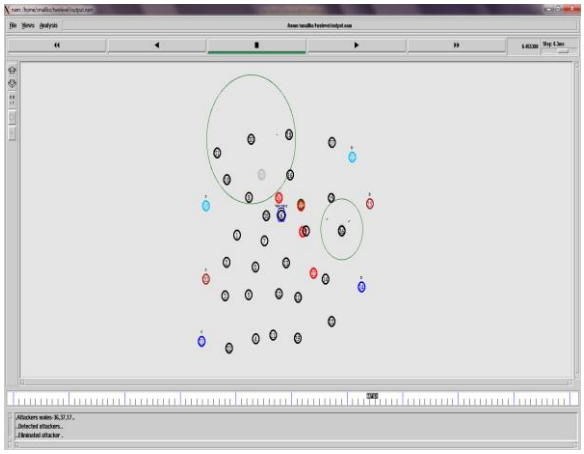


FIGURE 10: Representation of shortest path and simulation

5.4PERFORMANCEANALYSIS

Data transfer between the source and the destination nodes are sensed for the purpose of analyzing the performance of the network and to improve decision making.this simulation is exclusively done to enhance the performance of the system and to have a hazzle free data communication between nodes in the network.

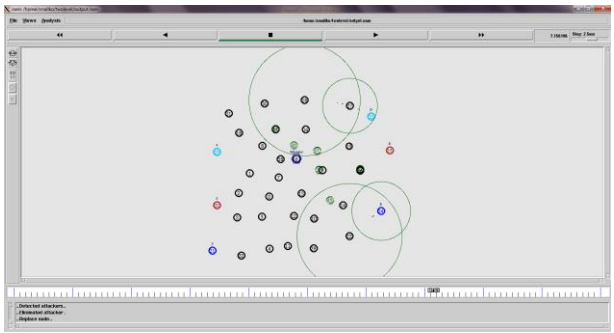


FIGURE 11: Snapshot of the performance analysis of sensor nodes

5.5 AVERAGE END TO END DELAY

The time taken for the packet to be transmitted across the network from source to target. It also considers the queue of the process and dealy that takes place in the route.

∑ (arrive time – send time) / ∑ number of connections.

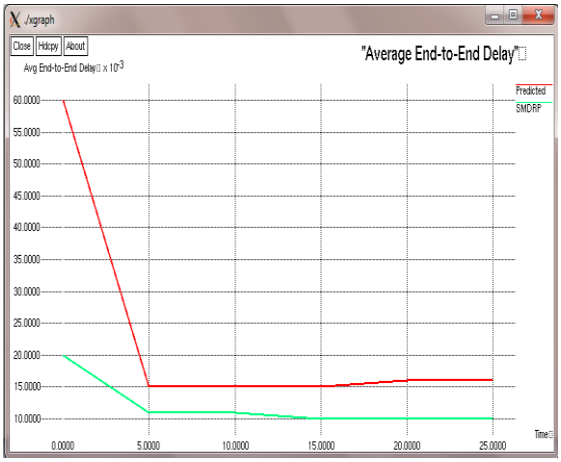


FIGURE 12:Comparision of average end to end delay of existing and proposed systems

5.6 **ENERGY LEVEL**

Batteries have limited or fixed capacity. Decisions are made based on energy consumption. Making use of energy for wireless nodes provides the exact output of the experiment.In general configuration of node performd in ns2 with the help of energy given is infinite .It directly indicates that no energy log that has been carried out.

6.CONCLUSION

Thus with the help of proposed system any low level attacks and DOS attacks made by the attacker are successfully identified and eliminated using Secure Multipath Routing Protocol.

The results of this simulation are captured by snapshots os ns all-in-one software and cygwin software.

7.REFERENCES

[1] Abror Abduvaliyev, Al-Sakib Khan Pathan, Jianying Zhou, Rodrigo Roman and Wai-Choong Wong, "On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks", *Communications Surveys & Tutorials, IEEE* ,vol 15,pp.1223-1237,2013.

[2] I. Khalil, S.Bagchi,C.N. Rotaru, "UnMask: utilizing neighbor monitoring for attack mitigation in multihop wireless sensor networks*", Ad Hoc Netw.*,vol 8, pp. 148–164, 2010

[3]A.PravinRenold,R.Poongodhai,R.Parthasarathy, "Performance analysis of Leachwith gray hole attack in Wireless sensor networks",*International conference on computer,communication andInformatics*,pp 1-4,2012.

[4] Guangjie Han. Jinfang Jiang. Wen Shen. Lei Shu. And Joel Rodrigues, "IDSEP: a novel intrusion detection scheme based on energy prediction in cluster-based wireless sensor networks", *IET Information Security journal*, vol. 7, Iss. 2, pp. 97–105, 2013.

[5] Zhen-wei Shen; Yi-hua Zhu, "An Ant Colony System Based Energy Prediction Routing Algorithms for Wireless Sensor Networks*", 4th International Conference on Wireless*

Communications, Networking and Mobile Computing, 2008. WiCOM '08.pp1-4, 2008.

[6] M.Tiwari, K.V.Arya, R.Choudari,"Designing Intrusion Detection to Detect Black Hole and Selective Forwarding Attack in WSN Based on Local Information", *Fourth International conference on Computer Sciences and Convergence Information Technology,* pp 824-828, 2009

[7] T.Meena,M.Nishanti,E.Kamalabalan,"Cluster-based mechanism for multiple spoofing attackers in WSN",*International Conference on Information Communication and Embedded Systems (ICICES)*,pp.1-5, 2014

[8] W.R. Heinzelman,A. Chandrakasan,H. Balakrishman, "Energy-efficient communication protocol for wireless microsensor networks", *Proc. Hawaii Int. Conf. System Sciences*,pp. 3005–3014, 2000.

[9] "*Evaluation of AODV and DSR Routing Protocols of Wireless Sensor Networks for Monitoring Applications*": Asar Ali ,Zeeshan Akbar, Master's Degree Thesis-(October 2009).

[10] Chen M., Leung V., Mao S., Xiao Y. and Chlamtac I *"Hybrid Geographical Routing for Flexible Energy-Delay Trade-Offs".* IEEE Transactions on Vehicular Technology, 58, 9, 4976-4988 (2009).

[11] Mohi, M., Movaghar, A., and Zadeh, P. M. *"A Bayesian Game Approach for Preventing DoS Attacks in Wireless Sensor Networks*". WRI International Conference on Communications and Mobile Computing, 2009.CMC '13. (Jan. 2009), 3, 507–511 (2013).

[12] Ssu, K. F., Wang, W. T., and Chang, W. C. *"Detecting Sybil attacks in Wireless Sensor Networks using neighboring information*". Computer Networks. 53, 3042–3056 (2009).

[13] www.nsnam.com

[14] Abror Abduvaliyev, Al-Sakib Khan Pathan, Jianying Zhou, Rodrigo Roman and Wai-Choong Wong, "*On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks"*, Communications Surveys & Tutorials, IEEE ,vol 15,pp.1223-1237,2013.

[15] "*Wireless sensor network attacks and security mechanism"* (ISSN 2157-0418)
D.Martins ; Comput. Sci. Dept., Univ. of Franche-Comte, Besançon, France ;
H. Guyennet.

[16] "*Wireless sensor network attacks:An overview and critical analysis"*A.Taybei and S.Berber(2015).