I.J. Information Technology and Computer Science, **2014, 12, 1-10**
Published Online November 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2014.12.01

A Security Scheme against Wormhole Attack in MAC Layer for Delay Sensitive Wireless Sensor Networks

Louazani Ahmed
Industrial Computing and Networking Laboratory, Computer Science Department, University of Oran, BP 1524 Oran, Algeria
Email: ahmedlouazani@yahoo.fr

Sekhri Larbi, Kechar Bouabdellah
Industrial Computing and Networking Laboratory, Computer Science Department, University of Oran, BP 1524 Oran, Algeria
Email: {larbi.sekhri, kechar.bouabdellah}@univ-oran.dz

***Abstract*—** The main objective of this paper is to secure a cross-layer, energy efficient MAC protocol (CL-MAC) dedicated to delay sensitive wireless sensor networks (WSN) for detecting and avoiding wormhole attack. CL-MAC protocol is the result of our previous research works for which the security aspects have not been taken into consideration during its design stage. To formally prove the importance of the proposed scheme, we provide a theoretical study based on Time Petri Net to analyse some important properties related to the devastating effect of the wormhole attack and its countermeasure on the CL-MAC operations. Also, we perform an experimental evaluation through the simulation using realistic scenarios in order to show the performance of the proposal in terms of energy saving, packets loss ratio and latency. The obtained results indicate the usefulness of the formal study provided in this work when applied in security context and confirm clearly a good performance of the proposed scheme against wormhole attack.

Index Terms —Wireless Sensor Networks, Wormhole Attack, CL-MAC Protocol, Cross- Layer Optimization, Time Petri Nets, TiNA Tool.

I. Introduction

Wireless Sensor Networks (WSN) are emerging as a new information technology field and a rich domain of active research involving hardware and system design, networking, distributed algorithms, programming models, data management, security and social factors. WSN are being employed in various real time fields like military, disaster detection and relief, industry, environmental monitoring, agriculture farming, etc. Due to diversity of so many real time scenarios, security for WSN becomes a complex issue and a major consideration to tack into account. For each implementation, there is different kind of possible attacks that requires different security levels and methods. The main challenge for performing an efficient security mechanism comes from WSN nodes resource constrained nature [1]. A sensor node is considered as a nano-computer with a processing unit, limited computational power, restricted memory, sensing unit, low bandwidth communication device and a limited power source (*battery*) [2] and [3]. The wireless nature of communication channels of WSN makes it much vulnerable face to multiple severe attackers (*DOS, Sybil, Sinkhole, Wormhole, selective forward, Black hole, etc.*) [4], [5], [6] and [7], so that any intruder equipped with a suitable *RF* antenna can intercepts the communication.

Among these attacks, a particularly devastating one is known as the wormhole attack that is difficult to detect because it doesn't inject abnormal volumes of traffic into the network [8]. In a wormhole attack, malicious nodes will tunnel the eavesdropped packets to a remote position in the network and retransmit them to generate fake neighbor connections, thus spoiling both routing and neighbor discovery protocols and weakening some security enhancements. According to [9], when there are more than two wormholes in the network, more than 50% of the data packets will be attracted to the fake neighbor connections and get discarded.

Therefore, severe constraints and demanding deployment environments of WSN make computer security for these systems a more complicated task than for conventional networks [10]. In designing a WSN security protocol, the list of the following challenges is not limited because each deployment environment has its own challenges, properties and goals. Incomplete list of various challenges can be given [11]:

- Resource efficient secure network services like neighbor discovery, network initialization, multi path routing, etc.
- Use of various cryptographic services like broadcast authentication and key management with light weight encryption mechanisms.
- Security mechanisms should be provided for all fundamental services such as data aggregation, cluster formation, secure location discovery, etc.
- Deployment environment nature which is in more cases hostile.
- Communication channel and communication model (multi-hop).

Copyright © 2014 MECS

Many other problems need further research works. One is how to secure wireless communication links against eavesdropping, tampering, traffic analysis and denial of service.

In this paper, we propose a security scheme for a cross-layer MAC protocol (CL-MAC) dedicated to delay sensitive WSN against wormhole attack. To prove the effectiveness of our approach, we provide both a theoretical model based on Time Petri Net and an experimental study through simulation of realistic scenarios. CL-MAC is the result of our previous works [12] and [13], where the security aspect has not been taken into account during its design.

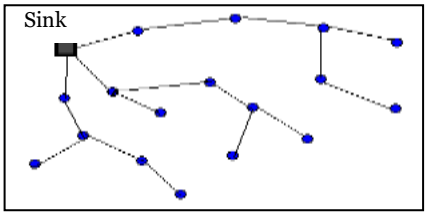
The remainder of the paper is structured as follows. Section 2 describes the wormhole attacks. Section 3 is an overview of the CL-MAC protocol and its vulnerability. In section 4, the proposed solution is discussed. Section 5 deals with a TPN formal modeling and analysis of the proposed solution. In section 6, experimental results are provided and discussed. Finally, a conclusion summarizes the paper and proposes directions for future work.

II. Wormhole Attacks

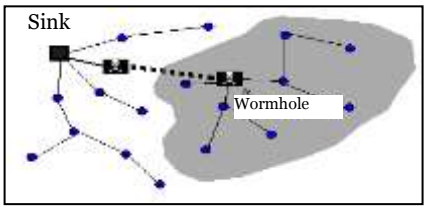
When the wormhole attack is present [14], [15], [16] and [17], a malicious node intercepts messages in one part of the network then tunnels them over a low latency link (wired link or a high RF band) and replays them in a different far away part of the network. A typical wormhole attack requires two or more attackers [18] - malicious nodes - who have better communication resources than regular sensor nodes [19]. Due to the nature of wireless transmission, the attacker can easily create a wormhole even for packets not addressed to it, since it can overhear them in wireless transmission and tunnel them to the colluding attacker at the other end of the wormhole. The tunnel can be established in many different ways, such as through an out-of band hidden channel (e.g., a wired link), packet encapsulation, or high powered transmission. The tunnel creates the illusion that the two end points are very close to each other, by making tunneled packets arrive either sooner or with lesser number of hops (short path) compared to the packets sent over ordinary routes. This situation allows an attacker to turn upside down the correct protocol behavior by controlling several routes in the network. Later, the attacker can use this to perform traffic analysis or selectively drop data traffic.

Wormhole attacks are classified dangerous and very difficult to detect especially in WSN using a routing protocol where routes are based on advertised information such as remaining energy, or an estimate of end-to-end reliability or minimum hop count to the base station.

Fig. 1 (a) illustrates paths formed by a network routing protocol in safe mode. Another network with the same topology and routing protocol, containing two working malicious nodes forming a wormhole attack is illustrated by the Fig. 1 (b). Packets communicated by any node within the colored area will be directed to a wormhole end node (malicious one). The simplest damage of such attack is to break the wormhole tunnel so that all nodes in the colored area will be disconnected from the rest of the network.



(a) Safe mode



(b) Weak mode

Fig. 1. Wormhole attack in network layer

Also it is independent from MAC protocols and immune to cryptographic techniques. The attacker doesn't need to know neither the MAC protocol operation nor how to decode encrypted packets to be able to replay them. In its most sophisticated form, the wormhole can be launched at the bit level or at the physical layer [21]. The replay process is done bit-by-bit even before the entire packet is received. In the latter, the actual physical layer signal is replayed. These forms of wormhole are even harder to detect since such replays can happen quite fast and thus they cannot be detected easily by timing analysis. The attack can also still be performed even if the network communication provides confidentiality and authenticity, and even if the attacker has no cryptographic keys. To distinguish these attacks from the simpler attack form where wormhole nodes copy the entire packet before transmittal through the wormhole link, we will refer to this simpler form of attack as store-and-forward attack following the terminology used in [20] and [21].

Once the wormhole nodes attackers have control of a link, they can do several things to actively affect the network operation.

As depicted in Fig. 2, *X* and *Y* denote the wormhole nodes connected through a long wormhole link. As a result of the attack, nodes in area *A* consider nodes in area *B* as their neighbors and vice versa.

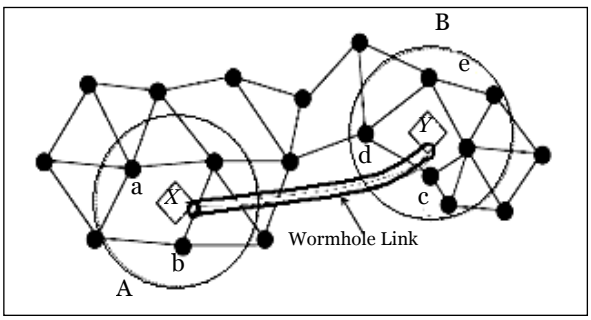


Fig. 2. MAC layer wormhole attack.

III. CL-MAC Overview and Vulnerability Study

CL-MAC is an energy efficient WSN cross-layer MAC protocol. As mentioned in [12] and [13], we have described the CL-MAC protocol and compared it with concurrent solutions. The two adjacent layers MAC and network exchange control information to find the shortest path to the sink so that all nodes belonging to the same path relying initiator node to the sink must be ready to rout packets at the right moment. Any other node which is a neighbor to one path-node that does not belong to the path has to turn off its transceiver from the beginning to the end of the routing process. The detailed CL-MAC algorithm can be found in [12].

CL-MAC protocol has a good behavior under the following conditions: A safe network, flat topology and using control information of two adjacent layers (network and MAC layers). These hypotheses on CL-MAC bring us to spell out its vulnerability:

- The hostile nature of the environment which wasn't taking into account by CL-MAC protocol.
- Security problems encountered in any other communication protocol.
- Difficulty to secure the communication channel.
- In CL-MAC, nodes within the same path must enter weak-up mode during the current communication, so no node will neither be disturbed by another communication nor inter in sleep mode. So a simple attack forces one node in current communication path to inter in sleep mode.

Despite the presence of multiple kinds of attacks in a network, anyone can break the basic protocol operation. So, for the CL-MAC, a simple passive wormhole attack causes several damages.

When neighborhood nodes exchange RTS and CTS packets to establish a communication in zone1 (see Fig. 3), a compromised node or an intruder one (forming a wormhole with another one far away) passively injects a copy of RTS/CTS packet far away in zone2.

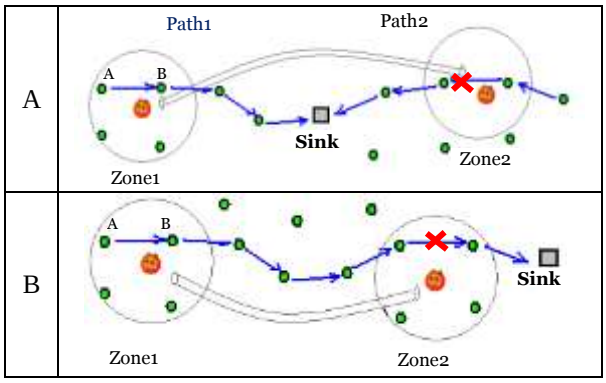


Fig. 3. CL-MAC Wormhole attack
(A): Wormhole joining two disjoined paths
(B): Wormhole in the same path

Whatever the placement of the two wormhole's ends nodes, either connecting two disjoined paths or two parts of the same path; the second attacker node in zone2 injects a copy of RTS packet which is not addressed to anyone of nodes in this zone (zone2). This situation leads all nodes within zone2 (second wormhole end's neighbors) to inter in sleep mode. Consequently the coming communication towards the sink will be blocked as shown in Fig. 3.

As mentioned in section I, a simple statistical study shows that 50% of the communications over two paths joined by a wormhole connection will be dropped.

IV. Proposed Solution

In [9], a wormhole detection mechanism to secure the AODV routing protocol in WSN using the Round Trip Time (RTT) technique is presented. The detection is based on message's RTT between successive nodes and their neighbor numbers. The consideration is that the adversary increases the number of the nodes' neighbors within the radio range, shortens the path and increases the RTT value between successive nodes. This proposed mechanism passes by three steps: construction of neighbor list for each node, searching the route between sources and destination node and finding the wormhole link location to make any necessary action.

In a typical wormhole attack, the attacker receives packets at one point in the network, forwards them through a wireless or wired link with much less latency than the default links used by the network, and then relays them to another location in the network. In this work, we assume that a wormhole is bi-directional with two endpoints although in theory, multi-end wormholes are possible. The attack may be passive, where packets are only reproduced far away from the neighbors' area or active where packets are reproduced and modified.

As depicted in Fig. 3, for the passive attack, we used the RTT mechanism to detect the presence of intruders in the nearby of both network layer (using route request and route replay) and the MAC layer when updating the neighbor list (by broadcasting hello message in the neighborhood). For the active attack, when even the packet header was modified so that it will reach a false destination during a communication between two neighbor nodes, we simply use a flag variable. This variable indicates on suitable packet reception as a reply to the initial message from the node which is involved in the current communication. A Black-List variable contains suspicious nodes' identifiers, it is used by a router node (a node place before the suspected node according to the path) to avoid infected path part and check for another alternative one. Whenever a node detects an attack in it's surounding, it broadcasts an alert message "AM" (Fig. 4 shows an alert message format). This alows both next and previous path nodes to update their Black-List (see Fig. 7).

Frame Control	ID (Faked node)	Alert Message	CRC

Fig. 4. Alert Message "AM" format

Copyright © 2014 MECS

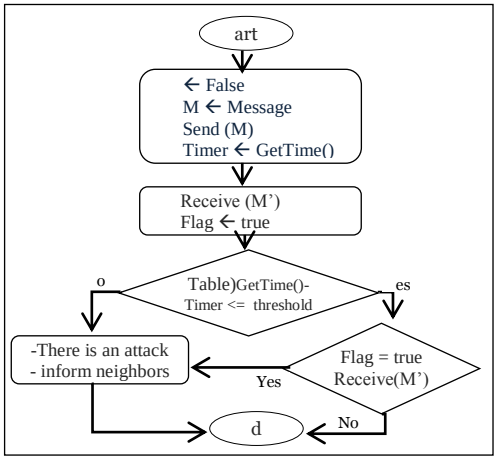


Fig. 5. Basic functions of proposed solution

Algorithm: Pseudo-code of Secured CL-MAC

```
1:  Algorithm Secured CL-MAC
2:    Input   : R-Table; // routing table
3:    Output  : AM;      // alert message
4:  Var
5:    Black-List, neighbors_list: id*;
6:    Flag    : Boolean;
7:    Timer   : time type;
8:  Start
9:    Built-Neighbors-List (Neighbors_list);
10:   Synchronize-the-Scheduler;
11:   Get-Routing-Table(R-Table);
12:  Repeat
13:    Flag ← False;
14:    M ← Construct-Message(R-Table);
15:    Send(M);
16:    Timer ← Get-Time();
17:    Wait;
18:    Receive(M');
19:   If ((Get-Time()- Timer)≤ threshold) Then
20:     Case Type-of-Message(M') Of
21:       Replay: If Flag Then
22:                 Goto X; //the second replay
23:               Else   // 1st message replay
24:                 Flag ← True;
25:               End-If
26:       Alert:  Update-Black-List;
27:        // Insert AM.ID into Black-List
28:     End-Case-Of
29:   Else
30:     X: There is an attack;
31:        AM ← Construct-Alert-Massage;
32:        Broadcast(AM);
33:        Halt-communication;
34:   End-If
35:  End repeat
36:  End-Algorithm
```

A. Detecting Wormhole Attack during Route Search and Neighborhood Discovery Operations

The mechanism of detecting wormhole attack is the same as discussed in [9] and summarized in the figure below(Fig. 6).

B. Detecting Wormhole Attack When Establishing a Communication

In this case, we define a flag variable associated to RTS packet. This variable is initialized to false, meaning that the sender node A is waiting for the CTS packet (see Fig. 3) coming from its interlocutor node B. when A receives the B's CTS packet, as a replay to its CTS one, it sets the flag variable to true and then sends the DATA packet. In a safe network operating, all nodes in the neighboring inter in sleep mode enabling nodes A and B to clearly communicate, and only four packets are exchanged (RTS, CTS, DATA and ACK). Assume knowing the presence of a wormhole attack (see Fig. 2 and Fig. 3). If it is a passive one, and this is the case of our study, the replication of the RTS packet in the other part of the network as depicted in Fig. 3-A will not affect the actual communication forwarding process on path1 (because RTS is a unicast packet), but any other communication passing by one node within zone2 will be stopped. The replicated RTS packet by the second end wormhole forces all neighborhood nodes in zone2 to inter in sleep mode, breaking down path 2.

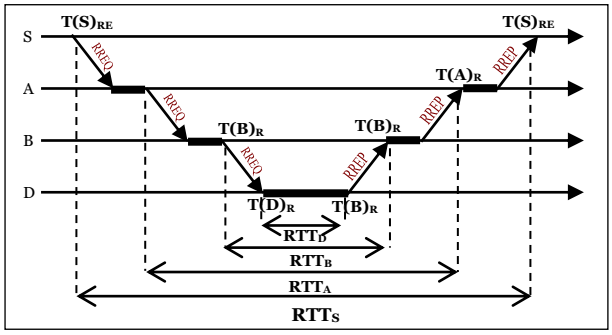


Fig. 6. Round trip time for finding route

When the attack is well placed on the same path like in Fig. 3 (b), the first wormhole end picks up the RTS packet in zone 1 generated by node A. Then the second end wormhole replicates it in zone2, so all nodes in this area enter in sleep mode conducting in a CL-MAC dysfunction case.

When the attack is active so that the destination filed header packet is changed in such manner it will be received by one node *C*, which is far away from node *A*, then *C* has to replay to *A* by sending to him a CTS packet (see Fig. 2). The time needed from receiving the CTS by *A* coming from *C* is greater than the time needed to exchange CTS and RTS packets between nodes *A* and *B*. When the node's *C* CTS packet reaches node *A*, this last one checks its flag if is set to true, in this situation the presence of a wormhole attack is detected. Node *A* decides to stop the communication and informs its neighbors that there is one end wormhole close to him by broadcasting an alert message "AM". Nodes receiving this AM message move node's *A* Id (the identifier of node *A* which is faked) from their neighbors lists to their Black-list, and stop forwarding packet to it (to node A) (see Fig. 7 below). According to Fig. 7, both nodes *B* and *D* add node's *A* Id to their Black-list. Then, node *B* will try to maintain communications from sources to the Sink avoiding neighborhood of node *A*.

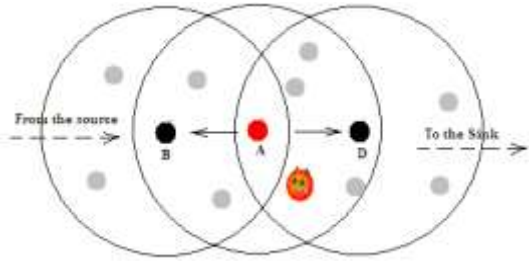


Fig. 7. Attack avoiding using AM message

C. Avoidance Wormhole Attack in CL-MAC

In secured CL-MAC protocol (SCL-MAC), avoidance attack mechanism is based on alert messages received by neighborhood nodes, especially the one preceding the detector attack node (node *A* in Fig. 7). The ID identifier of node *A* will be discarded from neighborhood list and added to Black-List. The updating process of routes is started automatically without taking into consideration the node *A*.

Fig. 8 below illustrates the functioning of avoidance mechanism of this kind of attack. The Fig. 9 shows the effect of avoidance mechanism.

NL: Neighbor List, F-ID: Faked node Identifier and AM: Alert Message.

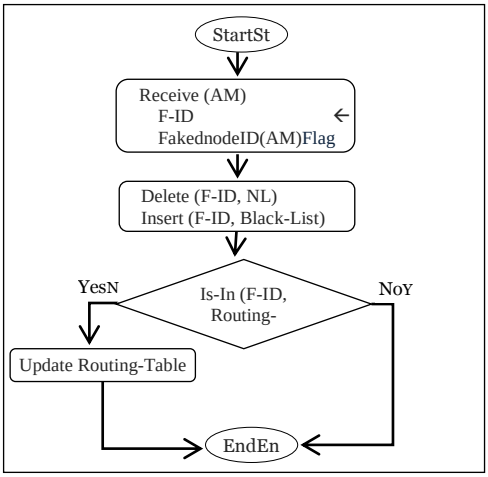


Fig. 8. Avoiding Wormhole attack

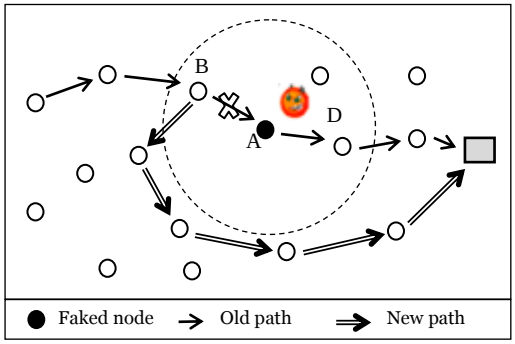


Fig. 9. Finding new path using avoiding mechanism

V. Formal Modelling

In order to formally verify the correct behavior of our proposed solution, we have chosen to model it in a suitable mathematical model according to its specifications. The time Petri nets (TPN) are attractable by their ability to easily model temporal constraints and the existence of the validation tools [22]. TiNA (Time Net Analyzer) is a software tool for TPN properties verification like boundedness, liveness, deadlock-freeness, etc. [23.] Fig. 10 illustrates a TPN model of our SCL-MAC protocol.

A. Model Hypothesis

SCL-MAC behavior hypotheses are as follows: we assume that *DIFS* duration = *SIFS* duration = 1 time unit, control packets *RTS*, *CTS* and *ACK* consume 3 time units each one, the *DATA* packet requires 10 time units for its transmission. Both the two wormhole ends take one time unit to transmit a packet from one part of the network to the other one far away using reserved channel (ultra frequency bound or wired link). Initially, only $p1$, $p8$, and $p17$ places are marked by one token meaning that the network is ready to start a new communication. M_0 means the start time after the network's deployment (ready state to establish the first communication).

$$M_0 = [p1, p8, p17]^t = [1,1,1]^t \quad (1)$$

Table 1. Description of the TPN Transitions of SCL-Mac Solution

Transition	Description
$t1$	*TRS packet generation* (*sender*)
$t2$	*DATA packet emission* (*sender*)
$t3$	*Enter in sleep mode* (*sender*)
$t4$	*Enter in weak up mode* (*sender*)
$t5$	*CTS packet emission* (*receiver*)
$t6$	*ACK emission* (*receiver*)
$t7$	*Enter in sleep mode* (*receiver*)
$t8$	*Enter in weak up mode* (*receiver*)
$t9$	*1st end wormhole node sends an RTS to 2nd end wormhole node*
$t10$	*2nd end wormhole node injects an RTS packet in the neighboring*
$t11$	*A 2nd end wormhole neighbor generates an CTS*
$t12$	*2nd end wormhole node routs the CTS towards the 1st end wormhole node*
$t13$	*1st end wormhole node injects in area A an CTS* (*the 2nd CTS injected in the surrounding of the area A*)
$t14$	*The 1st CTS reception by the sender*
$t15$	*The 2nd CTS reception by the sender* (*CTS routed from area B by the wormhole*)
$t16$	*Sender halts operating* (*wormhole attack detection*)
$t17$	*Node in area B , waits for no coming DATA packet*
$t18$	*Node in area B, enter in sleep mode*
$t19$	*Node in area B, enter in weak up mode*

Copyright © 2014 MECS

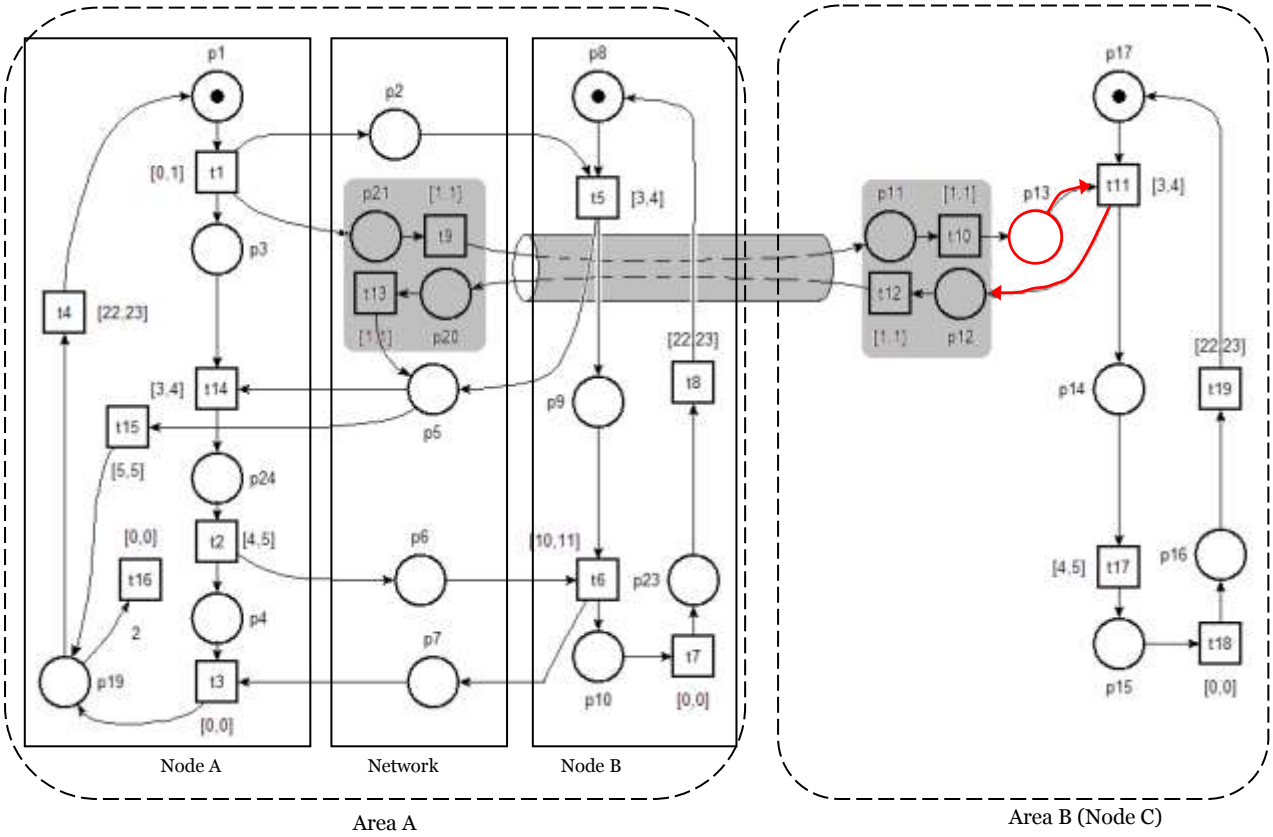


Fig. 10. Time Petri Net Model of Active and Passive Wormhole Attack (proposed solution)

B. SCL-MAC TPN Model

The meanings of transitions are given in table 1.

As illustrated in Fig. 10, each node in the WSN is represented by:

Sender: Transitions *t*1, *t*2, *t*3, *t*4, *t*14, *t*15 and *t*16. Transitions such *t*1 and *t*2 interpret the act of sending RTS and DATA packets respectively at precise moments modeled by the temporal intervals associated to the transitions (an RTS packet is sent after a DIFS and DATA packet is sent after reception of a CTS within 3 to 4 time units). Transition *t*3 allows node to enter in sleep mode after having received the ACK whereas *t*4 allows the token to remain in the place *p*19 (sleep state), time needed before starting the next communication. Transitions *t*14 and *t*15 model the flag associated to RTS packet, *t*14 allows the sender to transmit its DATA packet (flag = true) after receiving the first CTS from node *B* (see Fig. 10). Transition *t*15 depicts the act of initializing flag variable to false value when receiving another CTS packet from the net (it is generated by an intruder). The last transition *t*16 represents the behavior of the node *A* face to wormhole attack detection (node *A* turns off its transceiver just after broadcasting a message alert).

The two wormhole ends are modeled as:

First end wormhole (first intruder) in area A in Fig. 10: *t*9 and *t*13. *t*9 transition describes the tunneling of RTS packet from area A to area B. *t*13 describes the tunneling of CTS packet from area B to area A. *t*13 injects, in node A neighboring , the second CTS replaying to node A RTS. The reception of this faked packet by node A compels its flag variable associated to RTS packet to false value and then signaling the presence of a wormhole attack.

Second end wormhole (second intruder) in area B: *t*10 and *t*12. *t*10 introduce the RTS node's *A* packet coming in reality from area A into the area B. *t*12 transmit the CTS packet generated by a node in area B to node *A* in area A.

Place *p*19 receives the first token when the first intruder injects in the nearby of node *A*, the faked CTS packet coming from area B (second CTS). The second token is introduced in place *p*19, immediately after node *A* receives ACK packet. This place (*p*19) describes the node *A* sleep state. So, before the sleep time ended, transition *t*16 is fired and the place *p*19 was then left with zero token in so that the transition *t*4 will never be fired. This situation describes very well the act of isolating the node *A* from future communications, node *A* will be bypassed by creating new path over the area A (the wormhole will have no effects). Node *A* itself turns off its transceiver, in the TPN, node *A* will not be reinitialized again.

To distinguish between the two forms of wormhole attack (active and passive); we have designed two TPN models. The active attack is shown in Fig. 10 while the TPN model of passive attack is the same that in Fig. 10 without the red graph portion. To obtain a TPN model for passive wormhole attack, we discard the place *P*13, arrow *P*13→ *t*11 and arrow *t*11→ *P*12.

Attack detection can occur during exchanging RTS and CTS packets or when exchanging DATA and ACK packets (the mechanism is the same). This situation enables us to obtain a reduced TPN model illustrated by the Fig.11.

Copyright © 2014 MECS

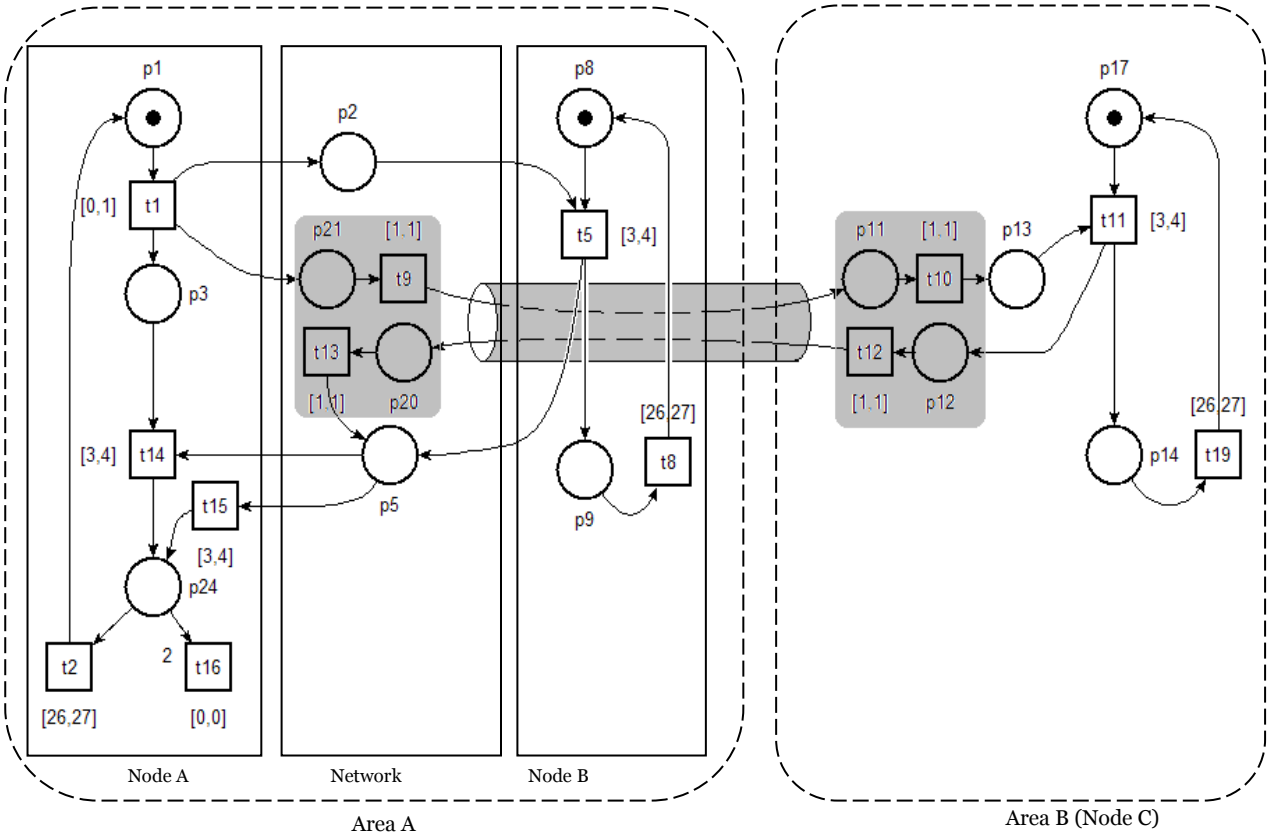


Fig. 11. Reduced TPN Model for SCL-MAC

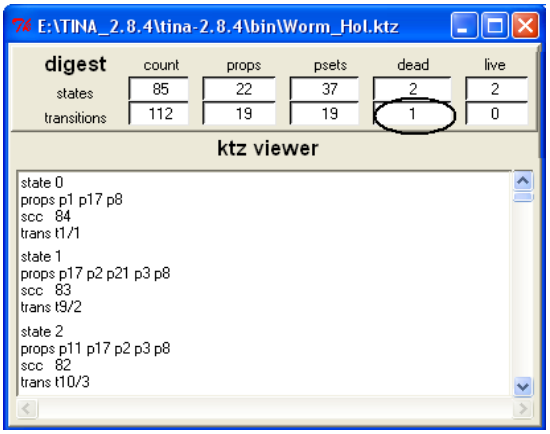


Fig. 12 (a)

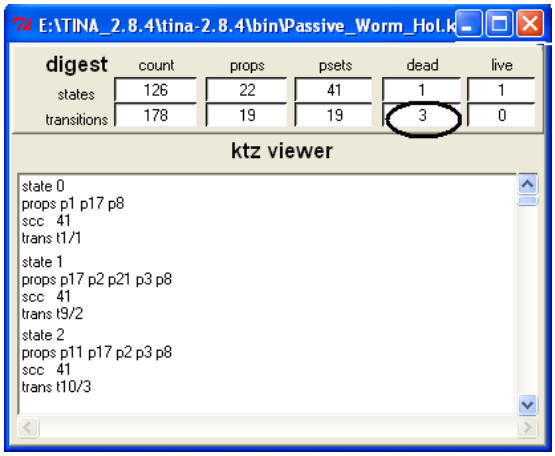


Fig. 12 (b)

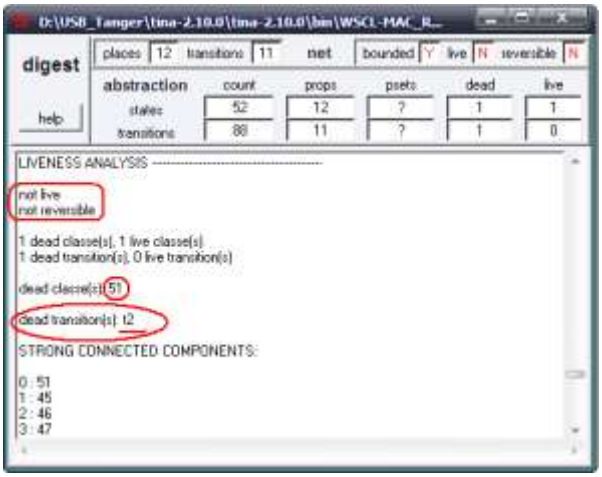


Fig. 12 (c)

Fig. 12. Reachability analysis CL-MAC solution using TiNA tool.
(A) Active wormhole, (B) Passive wormhole
(C) Reachability analysis for the reduced TPN

C. SCL-MAC TPN Model Results

The formal analysis of the obtained TPN model is carried out by comparing results given by TiNA software tool on the same model with (or without) the presence of the attack. In order to execute the model without the presence of wormhole tunnel, we have dropped the out coming arrow from *t*1 to *p*21.

Using TiNA tool, the reachability analysis shows the transition *t*4, in the presence of wormhole attack, as a dead transition preventing the re-initialization of the node

A (Fig. 12 (A)). In reality, this behavior reflects the isolation of the node from future communications. Neighbors nodes of *A* have to avoid routing packet to node *A* by finding alternatives path to the sink. Fig. 12 (B) shows that, in passive attack, the transitions *t*12, *t*13 and *t*16 are dead. Transitions *t*12 and *t*13 reveal that node *C* in area B will not reply to the RTC of the node *A* injected close to it by the wormhole, and then goes in sleep mode. When node *C* (belonging to another path bypasses zone B) sleeps it breakdowns that path for a while altering all communications over this path (see Fig. 3). Transition *t*16 is also dead; this means that node *A* and its neighbors are not affected by the presence of the wormhole.

VI. Experimental Results

In this section, we present simulation results of our algorithm using OMNET++ platform based Castalia simulator under parameters summarized in the table 2.

Table 2. Parameters Used for WSN Security Solution

Parameter	Value
Simulation Time	100 *secondes*, 500 *secondes*
Dimension of Area	30 *m*X30 *m*, 60*m*X60 *m*, 90 *m*X90 *m*, 120 *m*X120 *m*, *180 mX180m*
Number of Nodes	6, 10, 20, 30, 40, 50, 60, 70, 80, 90, 180
Sink Node	*Node* 0
Wormhole Nodes	*Node* 4, *Node* 5
Radio Module	*CC*2420
TX Power	-5*dbm*
MAC Protocol	*CL-MAC*

Many scenarios are used and implemented using Castalia simulator, from 30 deployed nodes in 30m X 30m area to 180 deployed sensor nodes in 180m X 180m area by calculating the variation in energy level on each sensor node.

A. Energy Wastage

We remark that the consumed energy increases with the network size in operating mode. Also, we remark in Fig. 16, the difference of energy wastage in safe and weak mode. In weak mode, the network expends more energy than in safe mode. This situation is due to packet retransmission and to path updating process.

Fig. 14 reveals that once the wormhole attack is far from the sink, the amount of consumed energy increases. This situation is explained by when the attack is closer to the sink and others neighbors, the consumed energy is smaller. Also, the consumed energy decreases when sending data and increases when the attacker is far from the sink. The starting process of finding new path surpasses the corrupted node in sending packets.

B. Packet' Lost Ratio (Safe Network versus Weak One)

Fig. 15 illustrates the packet lost ratio of both the two operating mode. It is clear that in safe mode, the number of lost packet is less than in the weak mode (in the presence of an attacker). Whenever the net size grows then the lost packet ratio increases, but we have less packet lost in safe mode.

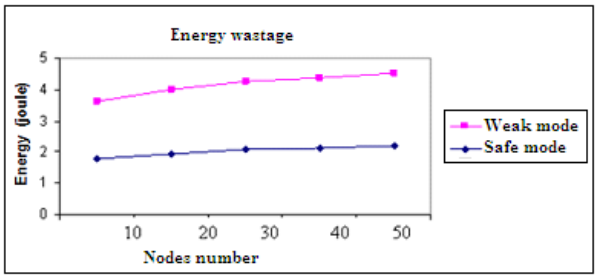


Fig. 13. SCL-MAC Energy wastage

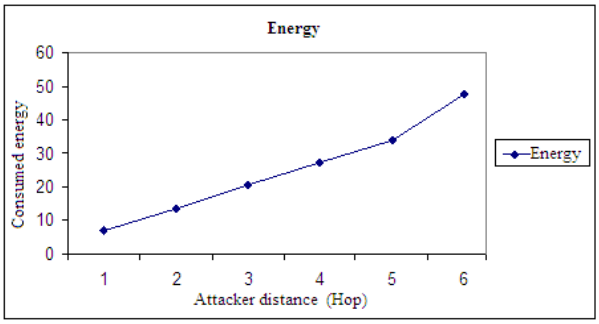


Fig. 14. SCL-MAC Energy consumption vs Sinkhole Attack distance

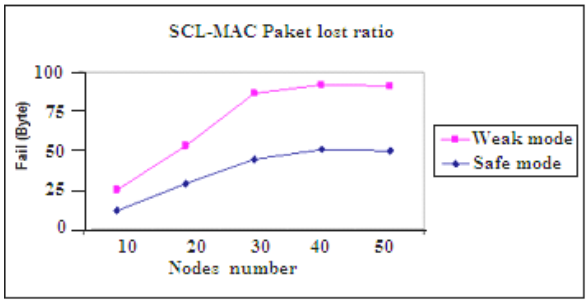


Fig. 15. SCL-MAC Lost packet ratio in both weak and safe mode

C. Latency

As depicted in Fig. 16, in weak mode, the latency (*T*) is greater than the one in safe mode (*t*) (*T* = *t* + *Δ time* unit). The time difference between the two latency mode "Δ" expresses the time spent by previous faked node (node B in Fig. 7) to update its routing table avoiding malicious node area and bypasses node A as in Fig. 8.

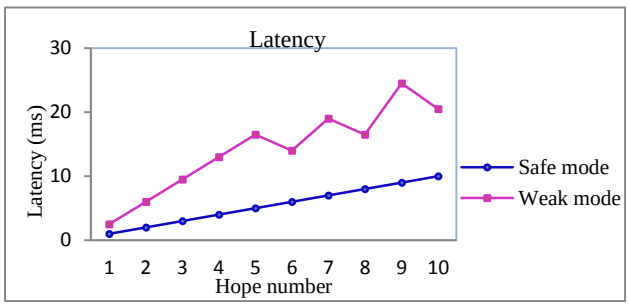


Fig. 16. SCL-MAC Latency

VII. Conclusion and Future Work

In this paper, a secured version of CL-MAC against wormhole attack has been presented. The proposed

solution is based on *RTT* approach. The *RTT* can be computed during the neighborhood discovery process at MAC layer or during the building of routing tables at the level of network layer.

We have proposed a time Petri net based approach to model the wormhole attack scenario and a detection mechanism. The formal analysis using TiNA tool allowed us to prove some properties of the TPN model. The obtained results showed clearly that the detecting wormhole attack and isolating node's neighbors at the one end from the network work well, thanks to the deadness property of the transition *t4*. This transition models the process of switching node *A* to weak up state and forces it to stay in sleep mode for a long period of time.

In order to strengthen theoretical results, we have implemented our proposed SCL-MAC algorithm using OMNET++/Castalia simulator to obtain empirical preliminary results in order to enhance TPN model properties. As future work, we try to secure our CL-MAC protocol against sinkhole attack.

ACKNOWLEDGMENT

This work was supported in part by the Industrial Computing and Networking Laboratory of Oran University.

REFERENCES

[1] K. Sharma and M.K. Ghose, "Wireless Sensor Networks Security: A New Approach", *In Proceedings of 16th International Conference on Advanced Computing and Communication (ADCOM 2008)*. Dec. 14-17, 2008, MIT Chennai.

[2] M. Meghdadi, S. Ozdemir and I. Güler, "A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks"; *The Institution of Electronics and Telecommunication Engineers (IETE)*, vol. 28, Issues. 2. pp 89-102, 2011.

[3] M. Yasir, "An Outline of Security in Wireless Sensor Networks Threats, Countermeasures and Implementations". Wireless Sensor Networks and Energy Efficiency: Protocols, Routing and Management Book, pp. 507-527, 2012.

[4] L. Hong, F. Hong and C. Fu, "Defending Against Wormhole Attack in OLSR". *Geo-spatial Information Science (Quarterly)*, vol. 9, Issue. 3, pp. 229-233, Sep. 2012.

[5] L. Kyuho, J. Hyojin and K. Dongkyoo, "Wormhole Detection Method Based on Location in Wireless Ad-hoc Networks", Book chapter in New Technologies, Mobility and Security. pp. 361-372, 2007. Springer.

[6] K. Roshan and V. Bibhu, Preventive Aspect of Black hole Attack in Mobile AD Hoc Network, *International Journal on Computer Network and Information Security (IJCNIS)*, June 2012 in MECS, 2012, 6, 49-55.

[7] C. Iwendi, A. Allen and K. Offor, "Smart Security Implementation for Wireless Sensor Network Nodes"; *Journal of Wireless Sensor Networks (JWSN)*, vol.1. pp. 14-26, July 2013.

[8] Y. Hu, A. Perrig and D. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks", *Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 3, pp. 1976-1986. April 2003, San Francisco, California, USA.

[9] Z. Tun and A. M. Htein, "Wormhole Attack Detection in Wireless Sensor Networks", *Proceedings of world academy of science, engineering and technology*, vol. 36. pp. 549-554 Dec. 2008.

[10] K. Sharma and M. K. Ghose. "Wireless Sensor Networks: An Overview on its Security Threats". *International Journal of Computer Applications (IJCA), Special Issue on "Mobile Ad-hoc Networks" MANETs,* pp. 42-45, 2010.

[11] J. Perrig, J. Stankovich and D. Wagner, "Security in Wireless Sensors network", Communications of the ACM. vol.47, No.6, pp. 53-57. June 2004.

[12] B. Kechar and A. Louazani, "CL-MAC: An Energy Efficient Cross-Layer MAC Protocol with Latency Improvement in Wireless Sensor Network". *17th International Conference on Computer Communication and Networks (ICCCN).* 3-7 Aug. 2008. Virgin Institute, USA.

[13] B. Kechar. L. Sekhri and M.K. Rahmouni, "CL-MAC: Energy Efficient and Low Latency Cross-Layer MAC Protocol for Delay Sensitive Wireless Sensor Network Applications". *The Mediterranean Journal of Computers and Networks*, vol.6, No.1. pp. 1-14, 2010.

[14] A. Suman, P. Saurabh and H. Verma, "A Behavioral Study of Wormhole Attack in Routing for MANET". *International Journal of Computer Applications (IJCA)*, vol. 26, No.10, pp. 42-46, July 2010.

[15] M. Garcia-Otero and A. Poblacion-Hernandez, "Detection of wormhole attacks in wireless sensor networks using range-free localization", *IEEE 17th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks Conference (CAMAD'2012).* Pp. 21-25, 17-19, Sept. 2012, Barcelona, Spain.

[16] P. G. Arfaat and A.H. Mir, "The Impact of Wormhole Attack on the Performance of Wireless Ad-Hoc Networks". *International Journal of Computer Science and Technology (IJCST)*, vol. 2, Issue 4, 2, pp. 421-425, 2011.

[17] P. Singh and D. Kaur. "An Approach to Improve the Performance of WSN during Wormhole Attack using Promiscuous Mode". *International Journal of Computer Applications (IJCA)*, vol.73, No.20, pp. 26-29, July 2013.

[18] R. Maheshwari, J. Gao and S. R. Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information", *INFOCOM 2007. 26th IEEE International Conference on Computer Communications*, pp. 107-115, May 2007, Anchorage, Alaska, USA.

[19] S. kumer, T.V.P. Sundararajan and A. Shanmugam, "Performance Comparison of Three Types of Wormhole Attack in Mobile Adhoc Networks". *International Conference on Information Science and Applications (ICISA).* pp 443-447, Feb. 2010, Chennai, India.

[20] M. Belkadi, R. Aoudjit, M. Daoui and M. Lalam, Energy Efficient Secure Directed Diffusion Protocol for Wireless Sensor Networks, *Int. Journal of Information Technology and Computer Science (IJITCS)*, 2014, 01, 50-56.

[21] A. Louazani, L. Sekhri and B. Kechar, "A Time Petri Net model for wormhole attack detection in wireless sensor networks". *4th International Conference on Smart Communications in Network Technologies (SaCoNeT)*, vol. 1, pp. 1-6, June 2013, Paris, France.

[22] B. Berthomieu and M. Menasche, "An Enumerative Approach for Analyzing Time Petri Nets". *IFIP Congress Series, Elsevier Science Publishers*, vol. 9, pp. 41-46. 1983, Amsterdam, Netherland.

[23] B. Berthomieu, P.O. Ribet and F. Vernadat, "The tool TINA - Construction of abstract state spaces for Petri Nets and Time Petri Nets". International Journal of Production Research, vol.42, No.14. pp. 2741-2756, 2004.

Authors' Profiles

Louazani Ahmed is a Ph. D candidate in Department of Computer science, Oran University; his current research includes Wireless Sensors Network Security and Protocols Modeling.

Sekhri Larbi is an Associate Professor at the Computer Science Department of Oran University. His current research area of interests include formal modeling in distributed and mobile systems, wireless ad-hoc and sensor networks, systems modeling using Petri nets, diagnosability and monitoring of automated production systems. He is member of the Industrial Computing and Networking Laboratory at Oran University. He has been a visiting professor at Cedric-CNAM research laboratory, in Paris, France, and Ecole Centrale de Lille (LAGIS) where he worked in Diagnosis of Industrial systems; and LIUPA Laboratory at the University of Pau, France; and distinguished lecturer at University of Ottawa, Canada.

Kechar Bouabdellah is an assistant professor in the Department of Computer Science at Oran University, Algeria. He has authored several journal publications, refereed conference publications and one book chapter. He has been a member of the technical program and organizing committees of several international IEEE/ACM conferences and workshops. He also serves as a referee of renowned journals. His current research interests include mobile wireless sensor/actuator networks, Zigbee/IEEE 802.15.4 technologies deployment, and heterogeneous wireless networks, with special emphasis on radio resource management techniques, performance modeling, provisioning QoS and practical societal and industrial applications.

How to cite this paper: Louazani Ahmed, Sekhri Larbi, Kechar Bouabdellah,"A Security Scheme against Wormhole Attack in MAC Layer for Delay Sensitive Wireless Sensor Networks", International Journal of Information Technology and Computer Science(IJITCS), vol.6, no.12, pp.1-10, 2014. DOI: 10.5815/ijitcs.2014.12.01