A Defense Strategy against Energy Exhausting Attacks in Wireless Sensor Networks

Djallel Eddine Boubiche and Azeddine Bilami
LaSTIC laboratory, Computer Sciences Department, UHL Batna, ALGERIA
Email: dj.boubiche@gmail.com, abilami@yahoo.fr

***Abstract*—One of the most challenging issues in wireless sensor networks is resilience against malicious attacks. Since energy is the most precious resource for these networks, Denial of sleep attacks is recognized as one of the most serious threats. Such attacks exhaust power supply of sensor nodes and can reduce the sensor lifetime from years to days. Authentication and encryption solutions have been proposed to protect the network from denial of sleep attacks. Though, the resources constraint motivates the use of simpler solutions to the same security challenges. In this paper, we survey different types of denial of sleep attacks and we propose a cross layer energy efficient security mechanism to protect the network from these attacks. The cross layer interaction between network Mac and physical layers is mainly exploited to identify the intruders' nodes and prevent sensor nodes from energy exhaust attacks. Simulation results indicate that our proposal is energy efficient and can significantly reduce the effect of denial of sleep attacks.**

***Index Terms*—Wireless sensor networks, Cross layer security, denial of sleep attacks**

I. Introduction

Securing wireless sensor networks (WSNs) adds more challenges to the research. This is because WSN properties make it harder to be secured than other types of networks. In WSNs, applying a high security level imposes more resource and decreases the energy efficiency of network.

Sensor networks are vulnerable to several malicious attacks. Since sensor batteries are severely limited, Denial of sleep attacks (DS attack) is recognized as one of the most serious threats. The DS attack [1] is a specific type of denial-of-service (DoS) attack that targets a battery-powered device's power supply in an effort to exhaust this constrained resource and reduce the network life time. Indeed, this attack tries to break in the device's power management system to reduce the opportunities to transition into lower power states.

Since Mac layer is responsible for managing the radio transceiver, defensive strategies implemented at this layer are the most effective in protecting radio usage. S-MAC protocol [2] represents the baseline energy-efficient sensor MAC protocol designed to extend WSN network lifetime. In this medium access control protocol, sensor node periodically goes to the fixed listen/sleep cycle. A time frame in S-MAC is divided into two parts: one for a listening session and the other for a sleeping session. Only for a listen period, sensor nodes are able to communicate with other nodes and send some control packets such as SYNC, RTS (Request to Send), CTS (Clear to Send) and ACK (Acknowledgement). Using a SYNC packet exchange, all neighboring nodes can synchronize together. Radios in networks which use this protocol will be asleep at 90% of the time, thereby producing an almost tenfold improvement in node life.

A denial of sleep attacker can manipulate Mac protocol and cause nodes to expend additional energy. For example, an attacking node in a SMAC-based network could repeatedly send request-to-send messages (RTS) and force the node listed in the RTS destination field to respond with a clear-to-send (CTS) message and remain awake waiting for the follow-on message. To provide a defense against this attack, most of existing researches propose authentication and encryption solutions or implement a complex and energy inefficient mechanisms. However, WSNs require simpler solutions to the same security challenges due to limited processing capability, memory storage, and energy capacity.

The purpose of this article is to discuss different types of DS attack and propose a defense strategy to protect the network from them. Our basic idea is the use of the cross layer interaction concept to prevent sensor nodes from energy exhaust attacks. In our proposal, the MAC layer uses the cross layer information (one hop routing table) from network layer in order to identify attackers. Then all received RTS packets are rejected if the sender does not belong to the routing path of receiver node.

Therefore attacked node doesn't stay awake to receive the follow-on message from the attacker node. In addition we compute RSSIs (Received Signal Strength Indication) of received packets and compare them with RSSI of neighborhood routing node to prevent network nodes from malicious denial of sleep attacks such as replaying attacks. Since we reuse the already available data generated by network, Mac and physical layers, our approach incurs very little additional cost and thus is ideally suited for resource constrained WSNs.

The remainder of the paper is organized as follows: In Section 2, we survey different types of denial of sleep attacks. Then, we present the existing security solutions in Section3. After that, we introduce our cross layer energy efficient security solution in Section 4. Section 5 illustrates the experimental results and discussion. Finally, we make conclusions and discus future work in Section 6.

doi:10.4304/jetwi.5.1.18-27

II. A SURVEY ON DENIAL OF SLEEP ATTACKS

Based on the attack strategy, we can classify denial of sleep attacks in six categories: sleep deprivation attack, barrage attack, synchronization attack, replay attack, broadcast attack and collision attack.

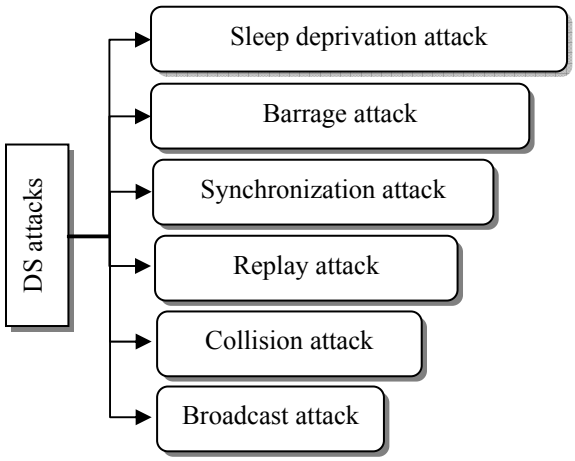

Figure 1. Proposed security mechanism algorithm.

A. Sleep Deprivation Attack

The Sleep deprivation attack is presented in [1], where target of the intruder is to maximize the power consumption of sensor nodes, so that their lifetime is minimized. By using lawful interactions, attacker node can keep the victim node out of its power conserving sleep mode. Thus, this attack can be used to dramatically reduce the lifetime of the victim. Further, this attack is difficult to detect given that it is carried out solely through the use of seemingly innocent interactions.

B. Barrage Attack

Barrage attack [3] causes its victims to spend more energy by bombarding them with legitimate requests. However, the purpose of these requests is to waste the victim's limited power supply by causing it to stay out of its sleep mode and perform energy intensive operations. In both the sleep deprivation attack and the barrage attack the victim will never enter its low power sleep mode. The difference between the two attacks is that the victim of a barrage attack will be actively performing work, whereas the victim of a sleep deprivation attack will, for the most part, remain idle.

C. Synchronization Attack

The goal of this attack [4] is to cause relative time synchronization problems at the MAC layer. The synchronization attack is simple but hard to detect as it stays within the confines of the protocol. In listen-sleep MAC protocols, each node maintains a listen-sleep schedule, and exchanges it periodically with neighbored node to synchronize their clock drift and form a virtual cluster. That allows them to listen and go to sleep at the same time. Updating schedule is accomplished by sending a SYNC packet. The SYNC packet is very short, and includes the address of the sender and the time of its next sleep. When a node receives a SYNC packet from another node on its same virtual cluster, it recalculates its next sleep time to maintain synchronization. Instead of simply resetting its next sleep time according to the value in the SYNC packet, the receiving node splits the difference between its next sleep time and the time in the received SYNC (T_{sleep_Sync}) packet as follows:

$$T_{sleep} = (T_{sleep} + T_{sleep\_Sync}) / 2 \quad (1)$$

The attacker can cause targeted nodes to stay awake for an extra fraction of the listen cycle by sending a compromised SYNC message at every SYNC exchange. Therefore attacked nodes extend their listen time based on the compromised sleep time extracted from received SYNC message. Presented simulation results show that under linear network topology, the attack can cause 30% more energy drain (due to loss of sleep and data retransmission) and 100% message loss (due to misalignment of the data periods).

D. Replay Attack

A replay attack is a breach of security in which information is stored without authorization and then retransmitted to trick the receiver into energy exhaust operations. In an unintelligent replay attack, recorded traffic is replayed into the network, causing nodes to waste energy receiving and processing these extra packets. If nodes in the network do not implement an anti-replay mechanism, this attack causes the replayed traffic to be forwarded through the network, consuming power at each node on the path to the destination. Undetected replay has the added benefit (to the attacker) of causing the network to resend data that could subvert the network's purpose. For example, replaying traffic in a military sensor network deployed to sense enemy movement could cause combat units to be misdirected.

E. Broadcast Attack

In this attack [5], attacker node broadcasts unauthenticated traffic into the network to reduce sensor nodes lifetime. Long messages can be broadcasted and must be received in full by all network nodes before the nodes discard them due to authentication failure. A subtle broadcast attack is one in which the attacker obeys MAC-layer rules of collision avoidance, thereby transmitting attack traffic only when there is no legitimate traffic in the network. This type of attacks is particularly hard to detect because it does not affect legitimate throughput, which might indicate an ongoing network attack.

F. Collision Attack

The collision attack [6] can be easily launched by a compromised (or hostile) node that does not follow the medium access control protocol, and cause collisions with neighbor transmissions by sending a short noise packet. In S-MAC, attacker checks the communication channel to ensure whether the medium is busy. If so, it assumes that the RTS/CTS or data packets are in the medium, therefore, it sends out jamming packets to collide with legal packets and form a collision attack.

III. Existing Security Solutions

One of the proposed defenses against energy exhaustion is to encrypt the control messages [7]. The authors propose the use of encryption and access control mechanisms provided for 802.11 MAC layer, which are known as Wired Equivalent Privacy (WEP). Using WEP, data is encrypted with a 40-bit RC4 algorithm and access points will authenticate stations by sending them encrypted challenge packets [8].

To prevent the denial-of-sleep broadcast attack, authors in [5] proposed a secured listen/sleep Mac protocol called G-MAC. In each cluster a gateway node is elected to collect cluster traffic and forward it out of the cluster. Authors assume that cluster nodes only respond to the gateway node, and unicast or broadcast messages sent to the gateway must be authenticated prior to being distributed to the individual nodes. Requests to broadcast traffic must be authenticated by the gateway node before the traffic can be sent to other nodes; therefore, only the gateway suffers power loss due to unauthenticated broadcast.

Three separate methods for mitigating the barrage and the sleep deprivation attacks have been analyzed in [3]: the random vote scheme, the round robin scheme, and the hash-based scheme. However the proposed solutions are designed for cluster based network and don't consider the other topology. In addition the authors assume that by scurrying the cluster head selection the network will be safe from sleep deprivation attacks. Though, an attacker node can target directly sensor nodes without attacking their cluster heads.

The authors in [4] introduced a threshold-based defense scheme to mitigate the effect of synchronization attack. The basic idea consists of ignoring all SYNC messages whose relative time to sleep is larger than expected clock drift threshold. Although this strategy might temporarily disable communication between the nodes, it will prevent the attack from propagating, and the two nodes will resynchronize during the next neighbor discovery phase. This strategy penalizes abnormal large clock drifts and sacrifices local communication to save global stability.

Another defense strategy against energy exhaust attacks is proposed in [9].The authors assume that attacker node should have some information of the victims (duty-cycle schedule) to perform energy depletion attacks. The authors introduce fake schedule switch scheme for counteraction. For collision attacks, receivers may not get the expected number of packets after they have send out CTS to the sender. So, if a receiver cannot get the expected packets or a sender do not receive any ACK after RTS for a Timeout Counter period, they can initiate a fake schedule switch. Namely, the victims and all their neighbors broadcast schedule switch SYNC but do not really change their schedule. And after a timer Timeout Back expires, they all come back to their former schedule and synchronization.

However, attackers will change their schedule and originate the measure algorithm to get the new duty cycle. So, the attackers will lose their energy quickly due to measurement and be border nodes of many virtual clusters. Though, the authors assume the attackers are equipped with limited power capability which is not always true. In addition the generation and the broadcast of the fake schedule can bring more extra overhead to the network and reduce the energy efficiency. [17, 18, 19, 20, 21].

A defense framework against denial of sleep attacks have been presented in [10]. The proposed defensive framework incorporates four key components: strong link-layer authentication, anti-replay protection, jamming identification and mitigation, and broadcast attack defense. Rainer Falk [11] proposed a secure wake-up scheme that entities of holding secret wake-up token can wake up a sleeping sensor node. Also, authors address the limitation of IEEE 802.15.4 communication standard to mitigate the sleep deprivation attacks. Sensor nodes are activated from a sleep state by a secure wake up radio only if messages from an authenticated and legitimate node are pending. Jingjun and Kendall propose a two-phase security system designed for hierarchical wireless sensor networks [12] and show how it can be used to detect Denial-of-Service attacks and track harmful intruders. An Artificial Immune System (AIS) approach and multiple-target tracking techniques are adopted to detect security threats in WSNs.

To prevent WSN from sleep deprivation attacks, authentication-based counter-measures are proposed in [13] for three topology maintenance protocols (PEAS, CCP, and ASCENT). Indeed, authors assume that neighboring nodes can establish pair-wise shared keys with each other. The pair-wise shared key is used for computing message authentication codes (MACs) for authenticating unicast messages exchanged between two neighboring nodes. Therefore, all communication between nodes is authenticated to prevent any intruders attack.

IV. Proposed Deffending Strategy

Most of studies presented previously bring more complexity to link layer protocols and are generally energy inefficient. Indeed it is not suitable to use energy inefficient security solutions to prevent sensors networks from energy exhaust attacks. Therefore we propose a simple and energy efficient security mechanism to preserve the network from different types of denial of sleep attacks. The new security mechanism is based on cross layer architecture that exploits interaction and collaboration of three adjacent layers in the OSI model i.e. network, Mac and physical layers.

The main goal of our security mechanism is to detect attacker nodes when they attempt to accomplish denial of sleep attacks and reject any packets sent from them. By using the routing information at the MAC layer, each sensor node knows previously the source of packets that will be received. Thus, any node trying to communicate (exchange controls or data packets) with the sensor nodes is immediately detected as an attacker if it is not included in the routing path.

To detect malicious kind of attacks such as replay attack, we combine the RSSI (Received Signal Strength Indicator) value [14] with routing information, to check the identity of the attacker node. At the initialization phase of communication the routing path is established and the RSSI value of the neighborhood routing node is computed and recorded. Then each node knows the signal strength of the packet sent by its neighbors. Therefore, the identity of the attacker node can be detected as the signal strength of the packets will not be equivalent to calculated RSSIs of neighborhood routing node. The following figure presents an example of the neighboring routing nodes information table of an attacked node N2 where its neighbor routing nodes are N1 and N3.

Neighboring routing nodes information of node 2	
Node id	***RSSI value***
id N1	RSSI N1
id N3	RSSI N3

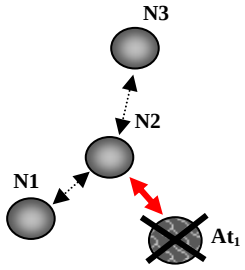

Figure 2. Example of neighboring routing nodes information table.

A. Defense Strategy Model

Network organization assumption:

We assume that: routing path, neighborhood routing tables, and neighborhood routing nodes RSSI value are computed centrally by the BS (base station). Then, at the set up phase each node sends to the BS, a control packet containing its identification, geographical position, and energy reserve. Since BS has knowledge of all nodes deployed in the collection field, it can identify any packet sent from intruder node. Therefore, the construction of routing path and neighborhood tables is secured. The proposed security mechanism can be applied to different listen/sleep Mac protocols; however we focus in this study to apply our security mechanism on SMAC protocol. We assume the same multi-hop routing protocol which we proposed in [15]. Also the SMAC synchronization schedule is sent only to the neighborhood routing nodes. All exchanged data packet must be preceded by an RTS and CTS packet, otherwise they will be rejected.

Analyzing the energy consumption of the proposed mechanism:

To evaluate the amount of energy consumed by our security mechanism we assume that attacker node attacks all nodes in the range of its radio antenna. Therefore the average number of attacked nodes by an attacker can be equal to:

$$A = (N-1)\,\pi\, r^2 / a \qquad (2)$$

Where, a is the area of the range region, N is the number of nodes in that region and r is the intruder transmission radius.

To estimate the total energy consumed by our security mechanism, we calculate the consumed energy to reject every denial of sleep attack.

$$ERi = E_{rx} + E_p \qquad (1)$$

Where ER_i is the energy consumed to reject the denial of sleep attack on node i, E_{rx} is the power consumption due to receiving of RTS packet from attacker node, and E_p is the power consumption due to processing of our security algorithm.

Then the amount of energy consumed by our security mechanism to defend the network from x attacker (at) nodes is equal to:

$$\sum_{at=0}^{at=x} \sum_{i=0}^{i=A} ERi \qquad (2)$$

Estimating the sensor life time with our security mechanism.

SMAC protocol divides network time into q frame time and separates each frame into active time and sleep time:

$$T_{Network} = q\, T_{frame} = q\,(T_{active} + T_{sleep}) \qquad (3)$$

We can compute the amount of energy consumed in each frame time by the following equation:

$$E_{frame} = T_{active}\,(E_{active}) + T_{sleep}\,(E_{sleep}) \qquad (4)$$

Where E_{active} is energy consumed during active state, and E_{sleep} is energy consumed during sleep state. since the energy consumed during active state is much higher than the energy consumed during sleep state, SMAC protocol sets the active time period to be very short period compared with the sleep time period (≈10% from time frame period) to conserve energy reserve.

The denial of sleep attacks affects the active period and extends it to be practically equal to the time frame. Then if the attacker node compromises a frame time, the energy consumed in this frame will be equal to:

$$\begin{aligned} E_{attacked\_frame} &= T_{active}\,(E_{active}) + T_{sleep}\,(E_{active}) \\ &= T_{frame}\,(E_{active}) \end{aligned} \qquad (5)$$

Therefore, if an attacker succeeds to compromise p frame time on a targeted node, the total of energy consumed by this node is estimated to be equal to:

$$E_{Total\text{-}unsecured\text{-}node} = (q\text{-}p)\,(E_{frame}) + p\,(E_{attacked\text{-}frame}) \qquad (6)$$

By using the proposed security mechanism, attacker node can't affect the active period and extent active state in the frame time. Therefore, the energy consumed by each node when an attacker node hits p frame time is equal to:

$$\begin{aligned} E_{Total\text{-}secured\text{-}node} &= (q\text{-}p)\,(E_{frame}) + p\,(E_{frame}) \\ &= q\,(E_{frame}) \end{aligned} \qquad (7)$$

With the previous definition we can estimate the life time of a secured and unsecured targeted node as follows:

$$Life\_time_{unsecured\text{-}node} = (C_{\text{-}battery}) / (E_{Total\text{-}unsecured\text{-}node}) \quad (8)$$

$$<<$$

$$Life\_time_{secured\text{-}node} = (C_{\text{-}battery}) / (E_{Total\text{-}secured\text{-}node}) \quad (9)$$

Where, $C_{\text{-}battery}$ is the battery capacity of the targeted node. By assuming that all network nodes have the same battery capacity, the average sensor lifetime across a network of n nodes was then calculated as follows:

$$AVG_{Life\_time\text{-}secured\_node} = (\sum_{1}^{n}(C_{\text{-}battery} / E_{Total\text{-}secured\text{-}node})) / n \quad (10)$$

B. Proposed Mechanism Behaviors under Denial of Sleep Attacks

In this section we analyze the behaviors of our security mechanism under different types of denial of sleep attacks..

Sleep deprivation attack:

In sleep deprivation attack, all nodes that receive an RTS packet must check the identity of transmitter node before they send CTS packets. Then, they reject the RTS packet and enter in the sleep mode if the transmitter node doesn't belong to the routing table. Otherwise, they send CTS packet and prolong their wake up stat to receive expected followed data. Contrarily to [7, 11, 12 and 13] we use a simple authentication scheme to verify the identity of the sender. Therefore we don't bring more extra load to network node and we optimize the energy efficiency. Figure 3 presents a sleep deprivation attack lanced by attacker 1 and attacker 2 to compromise nodes A and B. Also node A is unsecured where node B is secured with our proposed security scheme.

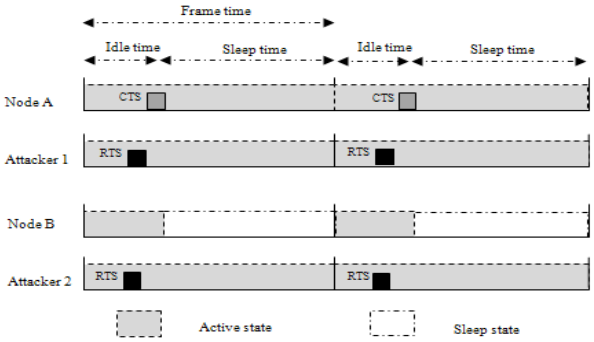

Figure 3. Sleep deprivation attack.

Barrage attack:

Like sleep deprivation attack, the targeted node is forced to stay awake, moreover it must perform energy intensive operations like receiving or transmitting data. By rejecting RTS packet sent from attacker node, proposed security mechanism deals with barrage attack and prevents targeted node to stay awake and performing any exhaustive task. Figure 4 shows the behavior of unsecured node (node A) and a secured node (node B) under the barrage attack.

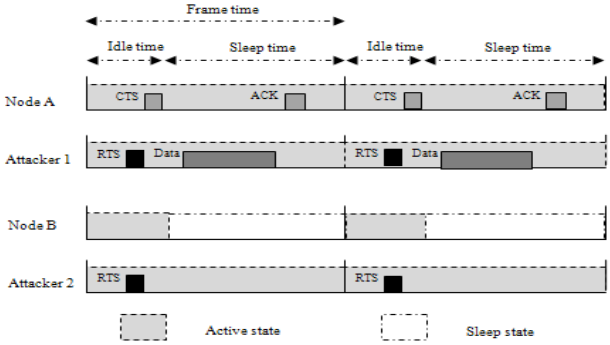

Figure 4. Barrage attack.

Synchronization attack:

The attacker node has knowledge of the Mac protocol, and sends SYNC packets crafted with arbitrary sleep Time values. Then corrupted SYNC sleep time is sufficient to keep targeted nodes awake. Since the SYNC message contains the identifier of the sender, receiver node can reject and ignore this message if the sender doesn't exist in the neighborhood routing table. Indeed, our security mechanism can provide the same performances result comparing with [4], furthermore it is more energy efficient than [9] as there is no extra overhead due to the fake schedule exchange.

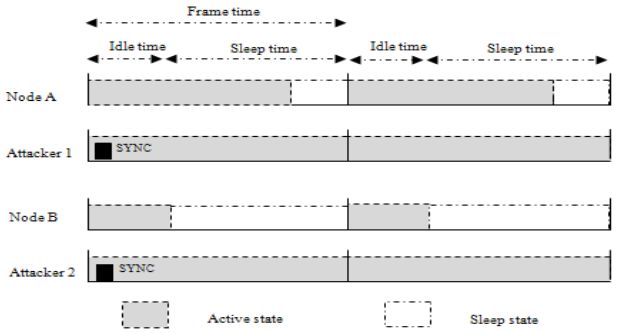

Figure 5. Synchronization attack.

Replay attack:

If attacker node replays any recorded traffic (RTS, SYNC...) it will be hard to distinct the malicious node from the normal one since they have the same identifier. Then, by combining RSSI value with neighborhood routing table, the proposed security mechanism can detect and mitigate replaying attack.

Broadcast attack:

We assume that the attacker node is malicious and it is hard to detect it. Therefore it has knowledge of the Mac protocol and obeys Mac-layer rules of collision, fragmentation, and communication schedules. The attacker node can broadcast a long message to all nodes in its radio range. Since in SMAC broadcast message there is no RTS packets that precede data message, the receiver node can't authenticate previously the followed broadcast message. Therefore, the authentication and encryption solution proposed in [7, 11, 12, and 13] can't prevent this kind of attacks since targeted node must receive broadcast message before it can be decrypted, which affects its sleep period and then drains the energy

reserve. The solution pro-posed in [5] mitigates the broadcast message; however it radically proposes a new Mac protocol. In our proposed mechanism, targeted node receives only the first data fragment and rejects remaining fragment (by entering in the sleep mode) of the broadcast message. Since the first fragment of the broadcast message contains the identity of sender, the proposed security mechanism can detect the intruder node and rejects then the followed fragment of broadcast message. Therefore, the effect of broadcast attack is significantly reduced as targeted node receives one fragment and does not prolong its wake up state to receive remaining fragments.

V. SIMULATION

A. Simulation Environment

Analysis of the performance of our intrusion detection is performed using the network simulator NS2. In this simulation, our experimental model is built on 100 nodes distributed randomly on a square surface of 100 x 100 m². The sensor nodes operate on non-renewable batteries and start the simulation by an initial energy equal to 2 J. Each node uses its limited reserves of energy throughout the duration of simulation, which involves the depletion of it. Thus, any node which has exhausted its energy reserve is considered dead. Therefore, it can't transmit or receive data.

To preserve their energy, sensor nodes will cycle in and out of a low-power sleep mode. The simulation parameters used in our simulation model are summarized in the table below:

TABLE1.
SIMULATION PARAMETERS

Parameter	Value
Surface of the network	100 m²
Location of the BS	(50, 75)
Number of nodes	100
Number of clusters	5
MAC layer protocol	SMAC
Initial duty cycle	10%
RTS, CTS, ACK size	30 Bytes
Traffic type	CBR
Routing Protocol	HEEP
Antenna type	Omni-Antenna

We assume a homogeneous network and a cluster based multi-hop routing protocol [15], where collected data is transmitted to clusters head throughout multi-hop routing path. The clusters formation, cluster head election and routing path creation are done in centralized way by the base station. We adopt the same energy consumption model proposed in [16], where the communication energy parameters are set as: Eelec=50nJ/bit, εfs=10pJ/bit/m^2, εmp=0.0013pJ/bit/m^4 and the energy for data aggregation is set as EDA=5nJ/bit/signal. The range of radio antennas is 2 meters.

SMAC protocol is used to access to the medium. A sensor node alternates between sleep mode and idle mode in each frame time. As SMAC default parameter, the idle time and sleep time are fixed to 143ms and 1289ms. Idle time is divided in two periods: SYNC time (88ms) and RTS/CTS time (55ms). A SYNC packet is sent every 10 frame cycle. The transmission bandwidth is set to 20kpbs, the latency of transmission and reception of a data packet is equal to 25µs, and the size of a data packet is 500 Bytes, with a packet header measuring 25 bytes.

In our simulation model, we assume that there are 5 attacker nodes randomly deployed in the well field. All attacker nodes pass through a period of passive listening and then try to attack nodes randomly targeted. All simulation results presented later are the average of 10 performed simulation operations. The duration of each simulation is set to 1000 sec.:

B. Simulation Results

First, we simulate the sleep deprivation attack and we measure the remaining nodes energy reserve, the number of dead nodes and the amount of data messages delivered to the BS every 100 seconds. We assume that attacker nodes target and attack randomly network nodes after being in passive state (120 seconds) and send every two frames time an RTS packet. In the passive state, attacker nodes try to capture the communication schedule of neighboring nodes and then synchronize theirs sleep deprivation attacks. Figures 6, 7 and 8 show the experimental results.

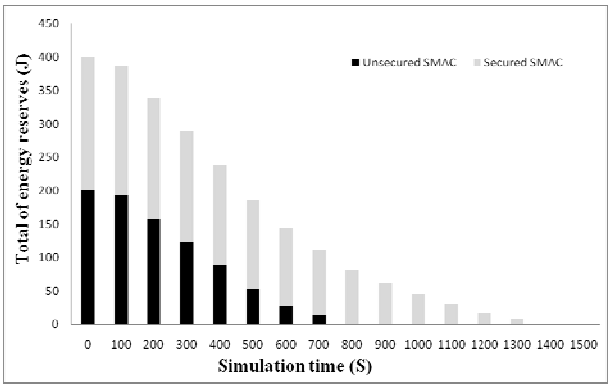

Figure 6. Total of energy reserves under sleep deprivation attack.

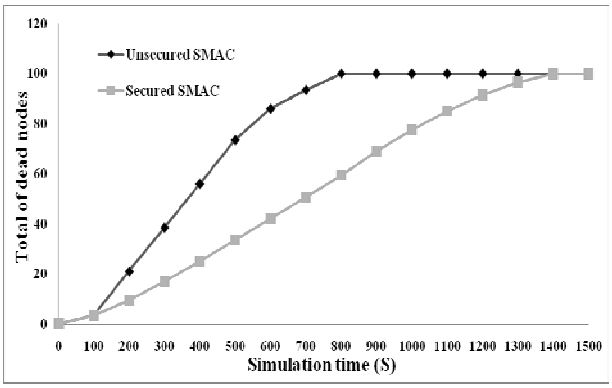

Figure 7. Number of dead nodes under sleep deprivation attack.

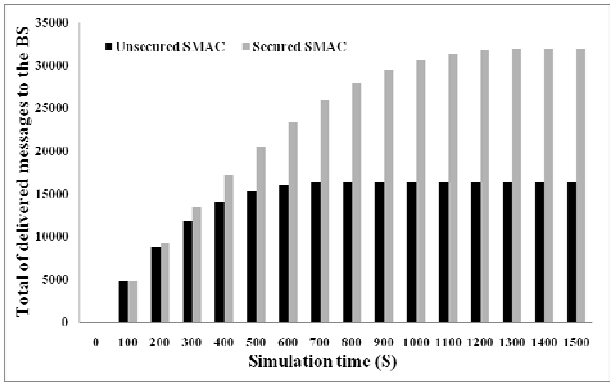

Figure 8. Amount of data messages delivered to BS under sleep deprivation attack.

Based on simulation results, we demonstrated that our security mechanism (secured SMAC) can prevent sleep deprivation attacks and preserve the energy reserve. Indeed, in our proposal network nodes consume regularly their energy reserve to transmit collected data. In the other side (unsecured SMAC), network node drain rapidly their energy reserve which reduce significantly the overall network life time.

To show the number of activated nodes in the network, we take a random snapshot of awaked nodes after 400 seconds of simulation time, which gives the result shown in Figure 9.

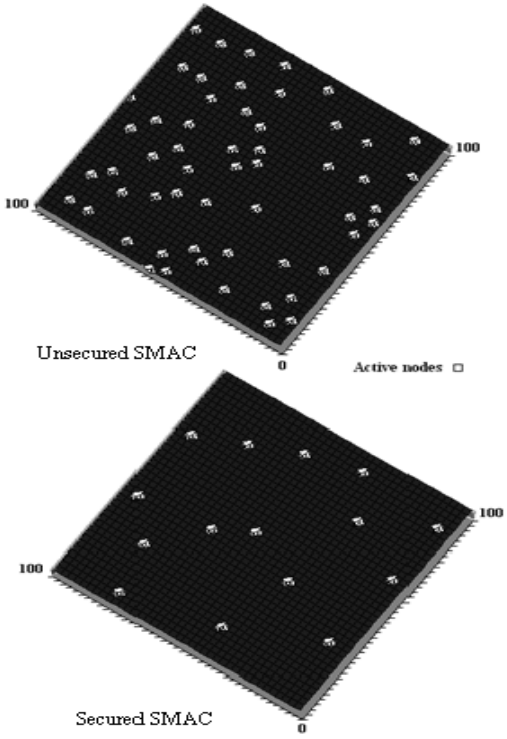

Figure 9. Activated nodes map under sleep deprivation attack.

We can clearly observe that the number of activated nodes in unsecured SMAC protocol is much higher than secured SMAC protocol.

In the next simulation, we analyze the behavior of our security mechanism under barrage attacks. We assume the same attacker characteristic detailed in the previous simulation, however the attacker node send a compromised data packet after the RTS packet to drain rapidly the energy reserve of targeted nodes.

As shown in Figures 10 and 11, the proposed security mechanism can protect net-work nodes from barrage attacks and prolong the network life time by 180 % compared with unsecured SMAC protocol. Indeed figure 12 shows that obtained delivered messages rate in secured SMAC protocol is more better then unsecured SMAC protocol.

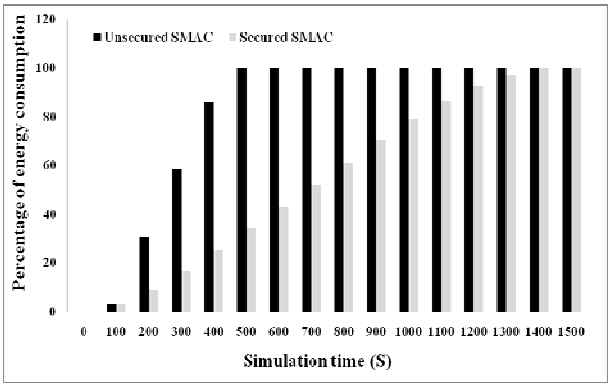

Figure 10. Percentage of energy consumption under barrage attack.

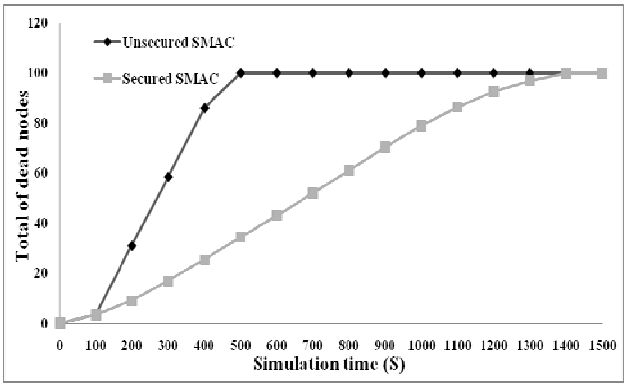

Figure 11. Number of dead nodes under barrage attack.

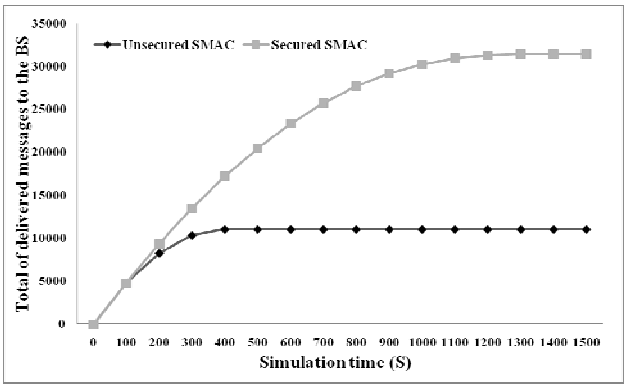

Figure 12. Amount of data messages delivered to BS under barrage attack.

To simulate synchronization attacks, we assume that attacker node send a compromised SYNC message at every two SYNC exchange (20 frame cycle). We measure then energy reserve, the number of dead nodes and the

amount of data messages delivered to the BS every 100 seconds of simulation time. Figures 13, 14 and 15 show obtained results.

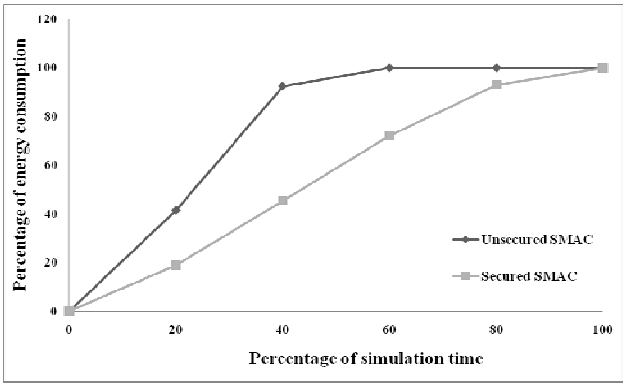

Figure 13. Percentage of energy consumption under synchronization attack.

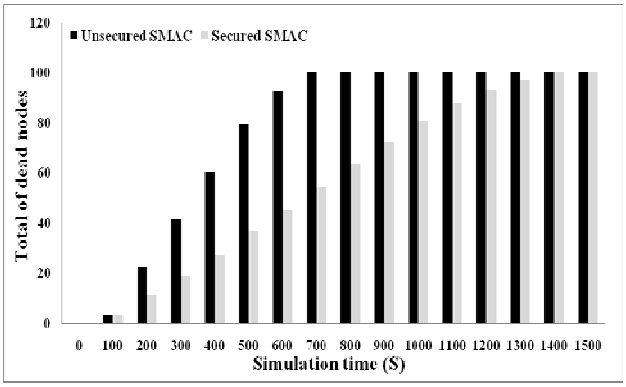

Figure 14. Number of dead nodes under synchronization attack.

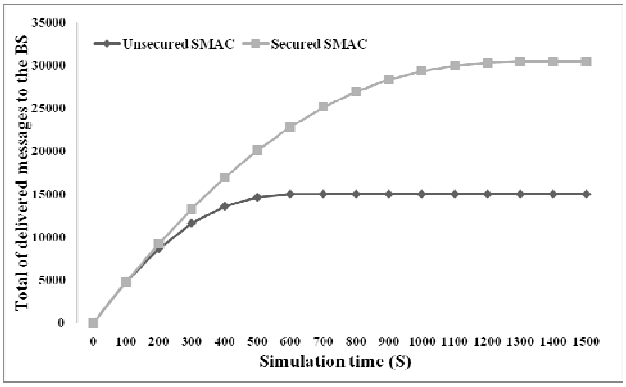

Figure 15. Amount of data messages delivered to BS under synchronization attack.

With unsecured SMAC network nodes drain rapidly their energy reserve due to the extra awaked time generated by the compromised SYNC message. However, our security mechanism rejects all suspected SYNC messages and preserves then network node from synchronization attacks.

The last experimental simulation consists of evaluating performance of the proposed security mechanism under broadcast attacks. Therefore we assume the same attacker characteristic used in sleep deprivation simulation. Also the attacker node targets all nodes in its radio range area (2 meters).

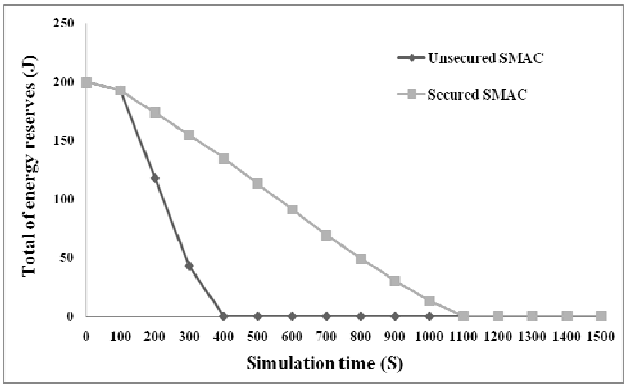

Figure 16. Total of energy reserves under broadcast attack.

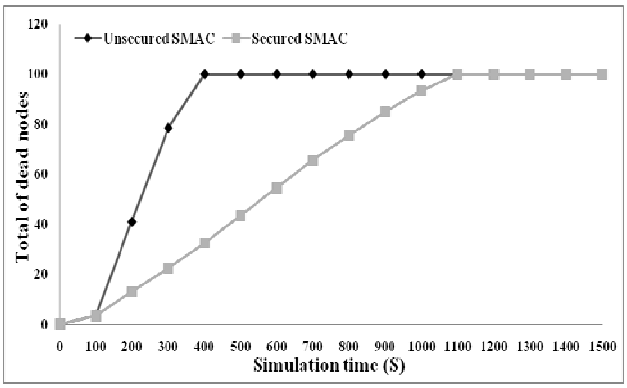

Figure 17. Number of dead nodes under broadcast attack.

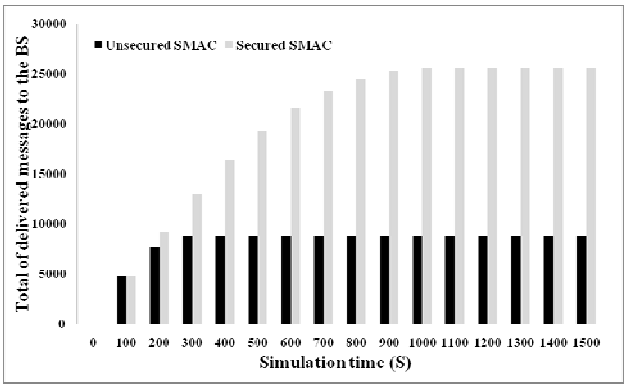

Figure 18. Amount of data messages delivered to BS under broadcast attack.

As shown in figures 16, 17 and 18, the broadcast attacks are the most harmful attack types that affect nodes energy reserve. Indeed our proposed security mechanism reduces significantly the effect of this attack. However, since targeted node must receive the first data fragment before it can identify attacker node, the network life time and the amount of messages delivered to the BS obtained under this attack is reduced compared with the other attacks. However, our proposed scheme outperforms over 150% the network life time obtained with unsecured SMAC protocol. .

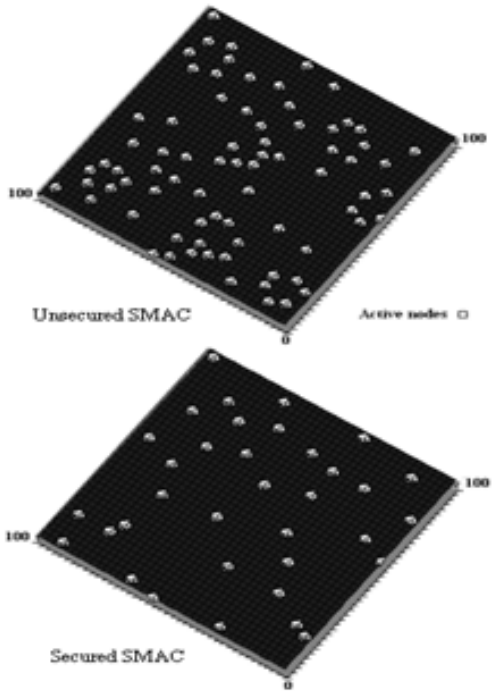

Figure 19. Activated nodes map under broadcast attack.

Figure 19 represents the awaked nodes map after 300 seconds of simulation time. In unsecured SMAC protocol over 70 % of network nodes are in active state to receive broadcast messages sent from attacker node, therefore the energy reserves are rapidly exhausted. However the amount of awaked node is significantly reduced by using the proposed security mechanism. .

VI. CONCLUSION

To secure network nodes from denial of sleep attacks, we proposed a cross layer energy efficient security mechanism where the cross layer interaction is heavily exploited. Our approach reuses mainly the already available data generated by network, Mac and physical layers to provide security scheme for network node. We don't claim that the proposed solution can prevent all types of denial of sleep attacks; though our proposal mitigates most of them. Simulation results demonstrate the performance provided by our security mechanism in terms of energy saving and network lifetime. As future work, we will try to analyze the behaviors of our security mechanism on other Mac protocol like TMAC and BMAC protocols.

REFERENCES

[1] F. Stajano, R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks," In ICISC, Springer-Verlag, 2000.

[2] Ye. Wei, J. Heidemann, and D. Estrin, "An Energy-Efficient MAC Protocol for Wireless Sensor Networks," IEEE INFOCOM, New York, Vol. 2, pp. 1567-1576, June 2002.

[3] M. Pirretti, S. Zhu, N. Vijaykrishnan, P. Mcdaniel, and M. Kandemir, "The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense," International Journal of Distributed Sensor Networks, 2: 267–287, 2006.

[4] L. Xiaoming, M. Spear, K. Levitt, N.S. Matloff, and S.F. Wu, "A Synchronization Attack and Defense in Energy-Efficient Listen-Sleep Slotted MAC Protocols," SECURWARE '08. Second International Conference on Emerging Security Information, Systems and Technologies, pp. 403-411, 2008.

[5] M. Brownfield, Y. Gupta, and N. Davis, "Wireless sensor network denial of sleep attack," In Proc. 6th Annu. IEEE SMC Inf. Assurance Workshop, pp. 356–364. 2005.

[6] Y.l. Law, "Link-layer Jamming Attacks on SMAC," Technical Paper, Univ. of Twente, NL, 2005.

[7] M. Stahlberg, "Radio Jamming attacks against two popular mobile networks," In Helsinki University of Tech. Seminar on Network Security, 2000.

[8] 3Com IEEE802.11b Wireless LANs Technical Paper.13p., referred 10.10.2000.

[9] C.C. Li, H.Q. Pei, and L. P. Ning, Qingquan, "An Effective Scheme for Defending Denial-of-Sleep Attack in Wireless Sensor Networks," Fifth International Conference on Information Assurance and Security. pp. 446-449. 2009.

[10] D.R. Raymond, R.C. Marchany, M.I. Brownfield, and S.F. Midkiff,, "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols," IEEE transactions on vehicular technology, VOL. 58, No. 1, pp. 367-380, January 2009.

[11] F. Rainer, and H. Hans-Joachim, "Fighting Insomnia: A Secure Wake-Up Scheme for Wireless Sensor Networks," Third International Conference on Emerging Security Information, Systems and Technologies, pp.191-196, 2009.

[12] J. Zhao, and K.E. Nygard, "A Two-Phase Security Algorithm for Hierarchical Sensor Networks," FUTURE COMPUTING 2011: The Third International Conference on Future Computational Technologies and Applications, pp. 144-120. 2011.

[13] A. Gabrielli, L.V. Mancini, S. Setia, and S. Jajodia, "Securing Topology Maintenance Protocols for Sensor Networks: Attacks and Countermeasures," IEEE Transactions on Dependable and Secure Computing, pp. 450 – 465, 2011.

[14] V. Bhuse, and A. Gupta, "Anomaly intrusion detection in wireless sensor networks," Journal of High Speed Networks, vol. 15, no. 1, pp. 33–51, 2006.

[15] D. Boubiche, and A. Bilami, "HEEP (Hybrid Energy Efficiency Protocol) Based on Chain Clustering," Int. J. Sensor Networks, Volume 10 Issue 1/2, pp. 25 - 35, 2011.

[16] W.R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Micro sensor Networks," IEEE Transactions on the wireless communications, Vol. 1, No 4, pp. 660-670, 2002.

[17] Nils Hoeller, Christoph Reinke, Jana Neumann, Sven Groppe. Dynamic Approximative Caching Scheme for Energy Conservation in Wireless. Sensor Networks. Journal of Networking Technology, 2 (1); p. 10-21.(2011).

[18] Chang Su, Lili Zheng, Xiaohai Si, Fengjun Shang. Low Overhead Geometric On-demand Routing Protocol for Mobile Ad Hoc Networks. Journal of Digital Information Management, 10 (2): pp. 114-120. (2012).

[19] Zouhair El-Bazzal, Khaldoun El-Ahmadieh, Ali Chamas Al Ghouwaye. Performance Enhancement of AODV Routing Protocol in Mobile Ad hoc Networks, Journal of Information Technology Review, 3 (2), pp. 47-57. (2012).

[20] Mande Xie, Guoping Zhang. The Design and Challenges of Online Reprogramming System for Wireless Sensor

Networks. Journal of Digital Information Management, 9 (6): pp. 255-260 (2011).
[21] Mohammadreza Balouchestani, Kaamran Raahemifar, Sridhar Krishnan. Robust Wireless Sensor Networks with Compressed Sensing Theory. Journal of Networking Technology, 3 (2): PP. 109-119. (2012).

Djallel Eddine Boubiche is currently a PhD student at the Computer Science Department,-University of Batna, Algeria He is a member of LaSTIC Laboratory. His research interests include wireless communication and sensor networks.

Azeddine Bilami is the director of LaSTIC Laboratory. He is currently serving as a Full Professor at the Computer Science Department at University of Batna, Algeria. His research interests are wireless and mobile networks, TCP/IP, internet, system on chip architectures; high performance interconnects for parallel architectures and multiprocessors.