Energy Efficient Security Mechanism for Black Hole Attacks in WSNs

Samir Athmani, Djallel Eddine Boubiche, Azeddine Bilami
Department of Computer Sciences, UHL Batna
LaSTIC laboratory
Batna, Algeria
{samir1904, abilami}@yahoo.fr, dj.boubiche@gmail.com

ABSTRACT: *Black hole is one of the most malicious attacks that target sensors routing protocols. The impact of this attack can be very harmful on hierarchical routing protocols. Several security solutions have been proposed to secure WSNs from black hole attacks. However, most of these solutions are complex and energy inefficient. In this paper we propose a hierarchical energy efficient intrusion detection mechanism, to protect sensor network from black hole attacks. Our approach is simple and based on control packets exchange between sensor node and base station. We have experimentally evaluated our system using the NS simulator to demonstrate its effectiveness in detecting and preventing efficiently the black hole attacks.*

Keywords: Wireless Sensor Networks, Intrusion Detection, Black Hole Attack, Energy Efficiency, Security, LEACH

Received: 10 May 2013, Revised 16 June 2013, Accepted 20 June 2013

1. Introduction

Security is one of principal obstacles of many applications in the wireless sensor network (*WSN*). Indeed, traditional security protocols are designed for resource powerful machines, and are not suitable for sensor networks. Routing data is a crucial task, and must be secured from malicious attacks. Hierarchical protocols are most efficient for routing data; however they are extremely vulnerable to routing attacks.

In hierarchical WSNs [1, 2, 3 and 4], network is typically organized into clusters, with cluster heads (CHs). The ordinary cluster members are responsible for sending data, while CHs node has better battery life, software capability, and hardware features. CHs are responsible for additional tasks such as collecting and processing data, and forwarding the results towards the base station (BS). Indeed, attacks involving CHs are particularly damaging, because CHs are responsible for critical functions.

One of the most devastating attacks that target cluster heads is the black hole attack [5]. A malicious node can be selected as cluster head, and absorbs all received data from its cluster members. Also, black hole attack can be created by a sinkhole attack [6]. The adversary node can position itself in the range of sink node, and attracts the entire traffic to be routed through it by advertising itself as the shortest route. Thus, the attacker absorbs any received message by rejecting and not forwarding it. Selective forwarding [5] is a particular type of black hole attack. Instead rejecting all received packets, adversary node selects randomly or maliciously packets that will be rejected.

Several researches have been proposed to prevent sensor network from black hole attacks. However, most of them are complex

and energy inefficient. In this paper we propose a hierarchical energy efficient intrusion detection system, to protect sensor network from black hole attacks. Our approach is simple and based on control packets exchange between sensor node and base station.

To detect black hole attacks, each sensor node must send periodically to the BS the number of packets sent to its CH. A second cluster head is selected to forward control packets to the BS. Finally, black hole table is maintained by each sensor node to prevent the selecting of malicious nodes as cluster heads.

The rest of the paper is organized as follows: In Section 2, we briefly survey existing security solutions. Then, we introduce our intrusion detection system in Section 4. Finally, we evaluate the performances of the proposed security solution in Section 5 and we conclude in Section 6.

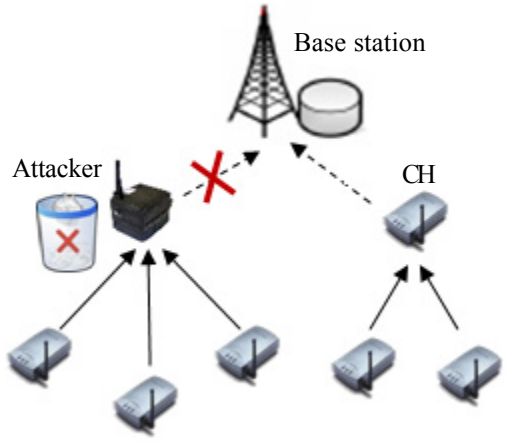

Figure 1. Black hole attack

2. Related work

The Black hole attack has been addressed by several researches in wireless sensor network. In this section we present a survey of these researches.

A security mechanism has been proposed in [7] for the black hole problem. The basic idea is to allow the intermediate node to send a reply message if it had a fresh enough route to the destination. However, the intermediate node could be a malicious node and could send route reply even if it had no fresh enough route to the destination to make a black hole attack. Therefore, authors proposed that the source node would send another route request to the next hop of the intermediate node to verify the authenticity of the route from the intermediate node to the destination node. If the route exists, from the intermediate node is trusted; otherwise, the reply message from the intermediate node is discarded.

Lightweight scheme for detecting selective forwarding and black hole attacks is proposed in [8]. To detect an eventual attack, authors propose to make nodes monitor their neighborhood and then communicate between each other to decide if there is an intrusion taking place. The scheme is further evaluated experimentally on a real WSN deployment. This scheme benefits from the neighbors monitoring so that there is a kind of distribution that will minimize the computation load on a detection agent node. However, there will be an increase in the communication messages between nodes during the collaboration for voting that will increase the communication overhead and as a result will deplete the power of nodes quickly.

An enhanced technique based on multi-path routing design is introduced in [9], to mitigate black hole attacks in the sensor network. This technique was called the Multicast Tree Assisted Random Propagation (MTRP). To transmit data from the SNs to the BS, authors propose the use of randomized routes, instead of using deterministic multi-path routes. A share is routed in the direction of the BS on a randomized path until it traverses a pre-specified number of hops to a forwarding node.

A hierarchical secure routing protocol called HSRBH, was proposed in [10] to detect and find a secure path against black hole attacks. To discover a safe route against black hole attacks, HSRBH uses only symmetric key cryptography. Most of black hole

attacks except the group leader collude with other nodes to make black hole attack. Therefore, it is much faster in detecting the black hole attacks, and the message overhead is very low.

The proposed protocol also provides the scheme to detect the black hole attack caused by the group leader colluding with other nodes. However, the solution is not scalable due to high computation and communication overhead. Also, public key cryptography is not feasible in sensor networks because of the capacities and constraints of the sensor devices.

Another security solution was proposed in [11], where sensor node performs power control to transmit a packet to more than one SNs, in the direction of the BS. If node that is on the forwarding path does not forward a packet, its next hop neighbor on the forwarding path will identify this event and report the BS as a black hole. This scheme is very expensive for a network with n black hole nodes, for each original message, $O(n)$ extra messages are required, which is very expensive.

In [12], authors proposed the use of multiple base stations for improving data delivery in the presence of black hole attacks. However, multiple base stations bring extra overhead and increase the communication and memory cost. Also, strategic position of the black holes is not considered; a black hole region close to the base station can capture all packets with high probability.

3. Proposed security solution

Our basic idea is to detect and prevent black hole attacks, by implementing an intrusion detection system based on a simple strategy. In our proposal, each sensor node sends a control packet to the base station at the end of transmission phase. Each control packet contains the node identifier (*id*), and the number of packets sent to cluster head (Nbr_{pk}). Then, base station compares the Nbr_{pk} of each node with the amount of packets received from its CH. That allows base station to detect an eventual black hole attack. In this case, base station will broadcast an alarm packet to all network nodes. The alarm packet contains identifier of black hole node (detected CH).

All sensor nodes maintain a black hole table, which contains identifiers of detected black hole nodes. Then, each sensor node checks its black hole table before the selection of its next cluster head. Which prevents that attacker node will be selected one more time as cluster head.

Sensor nodes can send their control packets directly to the base station; however, this can be energy inefficient and bring extra overhead to the network. Therefore, a second cluster head (*SCH*) is selected to transmit control packets to the base station. The choice of the SCH is simple, and based on node energy reserve. Therefore, node with the highest energy reserve will be selected as a second CH. Both CH and SCH selection are done in the setup phase of the communication protocol. Figure 2 presents the proposed IDS steps

Indeed, data aggregation can affect our security solution, since CHs aggregation deletes redundant packets and reduces the number of data sent to BS. To resolve this problem, CHs must add in the aggregated packet, identifiers of all nodes that sent data to the CH. Another problem situation is posed when the SCH is compromised (is a black hole node). However the BS will lance intrusion detection alarm, if it doesn't receive any control packet from the SCH. Therefore, we assume that all sensor nodes must send at least one data packet in each transmission phase.

Compared with the related IDS solution, our proposition is very simple and suitable for resource constrained sensor nodes. In fact the proposed IDS, doesn't use complex security mechanisms such as multipath routing, localization based or authentication and key distribution strategies. We propose a centralized based detection architecture, where base station is charged of analyzing and detecting anomalies behaviors. That reduces significantly the computation load on network sensor nodes.

The probability of black hole detection depends on number of black hole nodes (Nbr_{BH}) in the cluster and probability of a missed detection. In our IDS the black hole node can be not detected only if the BS doesn't receive any control packet from SCHs. Then the probability of a missed detection is equivalent to the probability of a collision occurring between SCH and the other clusters nodes.

Based on the Binomial rule, we can define the probability of detection of black hole node in a cluster as:

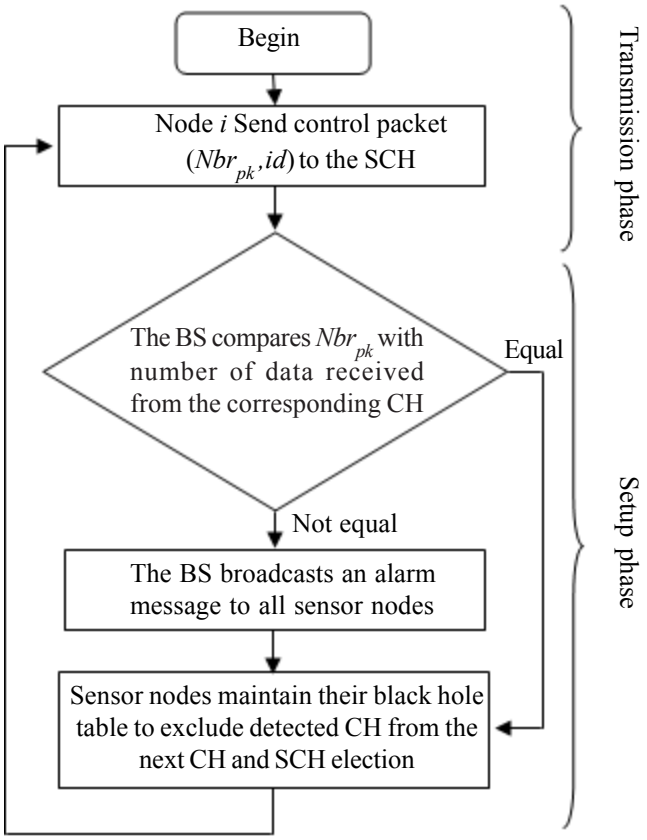

Figure 1. Proposed intrusion detection scheme

$$P_{BH} = \binom{Nbr_{BH}}{1} (1 - P_{Collusion}) P_{Collusion}^{Nbr_{BH} - 1} \quad (1)$$

Basing on equation 1 we can calculate the probability of detecting X intruder in the cluster:

$$P_{BH} = \binom{Nbr_{BH}}{1} (1 - P_{Collusion})^{X} P_{Collusion}^{Nbr_{BH} - X} \quad (2)$$

The majority of related security solutions are too expensive for sensor network. Since energy is the most precious resource, security mechanisms should be simple and energy efficient. Indeed, multipath routing, localization based and cryptographic strategies are energy inefficient and bring extra overhead to the network. Therefore we propose a simple and energy efficient security mechanism to preserve the network from black hole attacks.

Our IDS introduces a little energy consumption compared with other security mechanisms. The additional energy load is due to the periodic exchange of control packets between sensor nodes and base station.

To estimate the total energy consumed by our IDS, we calculate the node energy consumption on every communication round (setup and transmission phases).

$$E_{Round} = E_{tx} + E_{BH\_Table} \quad (3)$$

Where: E_{tx} is the energy consumed to transmit control packet to the SCH, and E_{BH_Table} is the energy consumed to maintain the black hole table.

Then, the total energy consumption is equal to:

$$\sum_{i=0}^{i=Nbr\_round} E_{Round} \quad (4)$$

Where: $Nbr_{\_round}$ is the total of communication round. The energy consumed to transmit control packet to the SCH can be computed by the following equation:

$$E_{Round} = \sum_{j=1}^{j=M} \sum_{i=1}^{i=N} (q_i E_{elect} + q_i E_{fs} d^{2}_{toSCH}) \quad (5)$$

Where: q_i is the size of the control package transmitted by the node i, E_{elect} is the power consummated by electronic circuits (computation energy), E_{fs} is the energy lost in the space of transmission, d_{toSCH} is the distance between node i and the SCH, N is the number of alive nodes in the cluster, and M is the number of clusters in the network.

Also we can compute the E_{BH} energy by the given equation:

$$E_{BH} = aE_{elect} \quad (6)$$

Where: a is the size of the alarm packet. Indeed the E_{BH} is the energy consumed to receive an alarm packet from base station.

4. Simulation

4.1 Simulation environment

The performance of our intrusion detection system is analyzed through the network simulator *NS*2. Our experimental model is built on 100 nodes distributed randomly on a square surface of 100×100 m^2. To evaluate efficiently our protocol, we assume a heterogeneous sensors network. Then 90 sensor nodes are initialized with 2 joules of energy, while the other 10 nodes are initialized with 200 joules. Simulation parameters are summarized in the table below:

Parameter	Value
Network surface	100 m^2
BS location	(50,75)
Number of nodes	100
Number of clusters	5
Size of data packet	500 Bytes
Size of packet header	25 Bytes
E_{el} (compute energy)	50nJ/bit
εfs (propagation energy)	10nJ/bit/m²
Number of attacker nodes	10
Size of information packet	128 Bytes
E_{DA} (aggregation energy)	5nJ/bit/signal
Routing protocol	LEACH
MAC protocol	TDMA
Traffic type	CBR

Table 1. Simulation Parameters

LEACH protocol is used to organize the network in a hierarchical cluster based topology. Indeed, the proposed IDS can be implemented on any hierarchical routing protocol, however we firstly choose to experiment it on LEACH, since it is one of the basic hierarchical routing protocol. We adopt the same energy consumption model proposed in [1]. The transmission bandwidth is set to 20kpbs, the latency of transmission and reception of a data packet is equal to 25μs.

We assume that there are 10 attacker nodes randomly deployed in the field. Two types of black hole attacks are defined. In the first type (*simple black hole*), attacker node is simple and initialized with 2 joules of energy. The second type (*malicious black hole*) uses a malicious attacker node, which has high energy reserves (200 *joules*). Therefore attacker node will be selected many times as a cluster head, which leads to more black hole attacks. All simulation results presented later are the average of 10 performed simulation operations. The duration of each simulation is set to 1000 sec.

4.2 Simulation results

Our IDS performances are analyzed against black hole and selective forwarding attacks in terms of: amount of data messages delivered to the base station and energy efficiency.

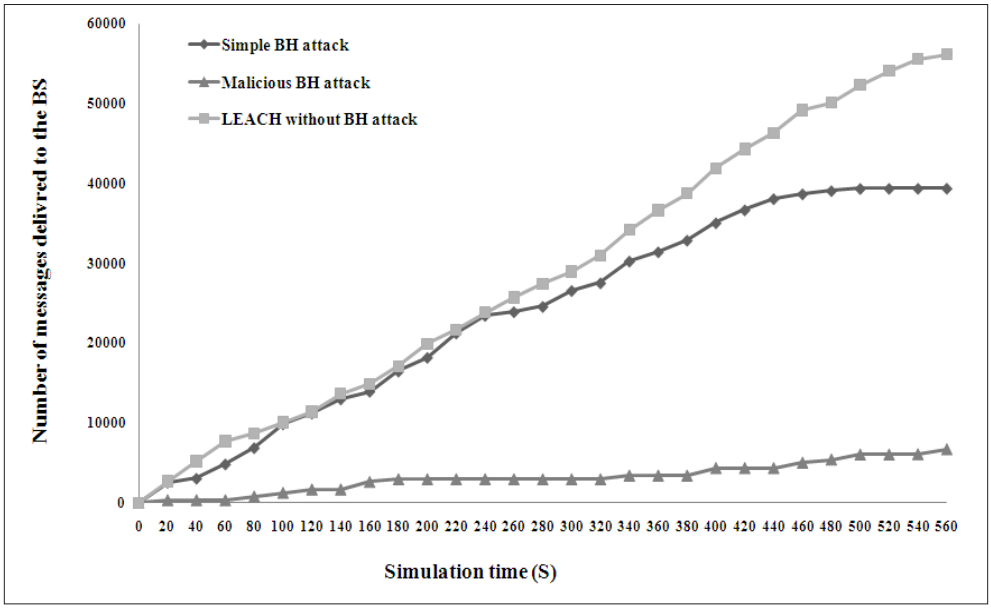

Figure 3. Number of data messages delivered to BS under black hole attack

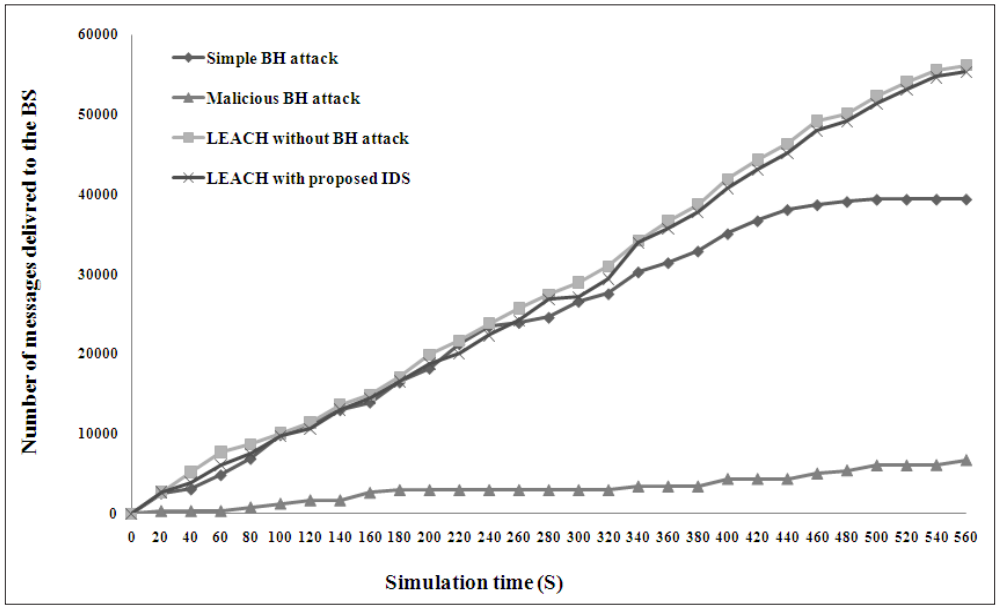

Figure 4. Proposed IDS under black hole attack

4.2.1 Black hole attack

First, we measured the number of data messages delivered to the base station, under simple and malicious black hole attacks.

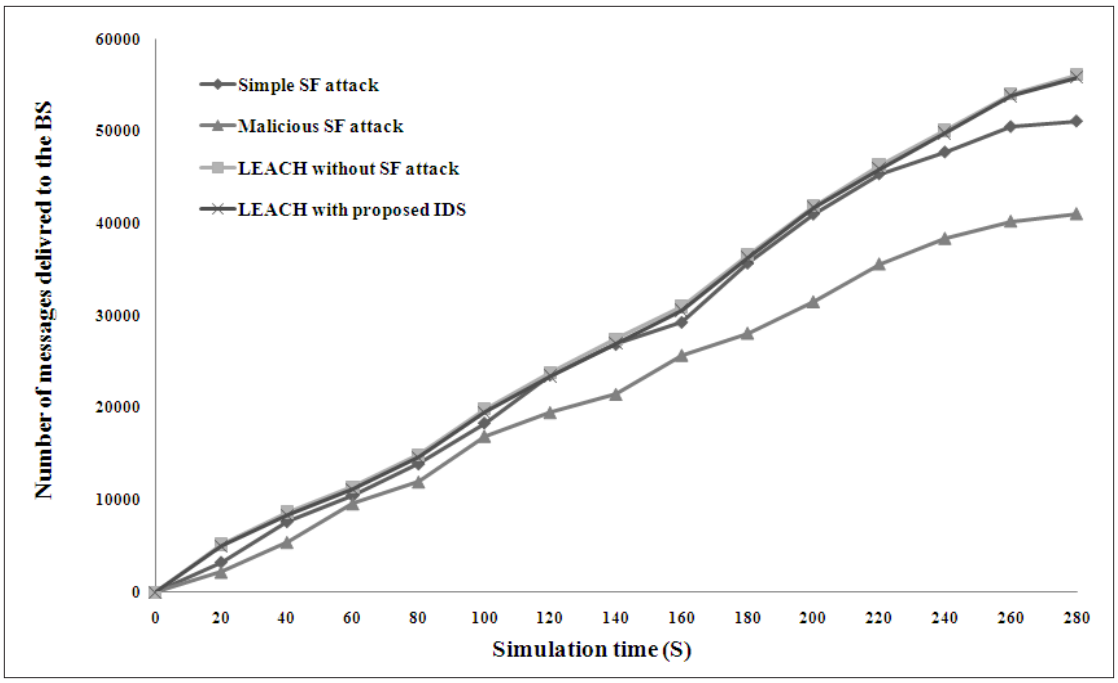

Figure 5. Proposed IDS under selecting forwarding attack

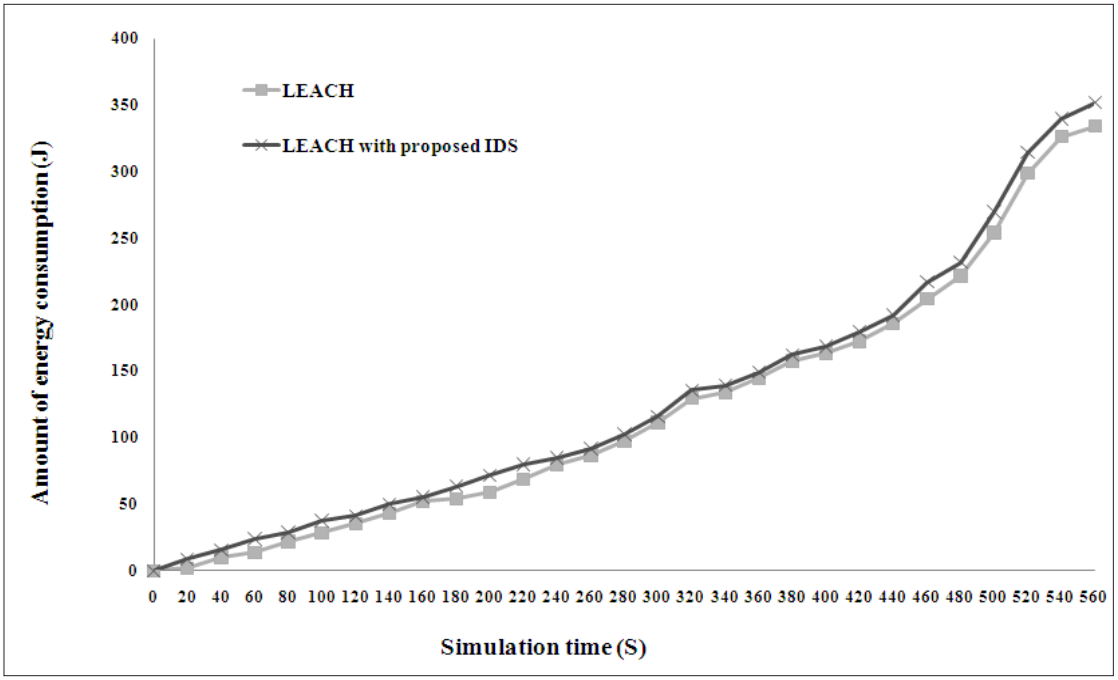

Figure 6. Energy consumption of the proposed IDS

The following figures show the results.

We can clearly observe that the simple black hole attack reduces the amount of data sent to BS by 30 percent. However the malicious black hole attack has more devastating impact, since it reduces the number of data packets by more than 88 percent. Indeed CH role rotation adopted by LEACH protocol doesn't mitigate the malicious black hole attack, since black hole node will be selected most probably in the next communication round. In the next simulation, we compare results obtained with our IDS against simple and malicious black attack.

Based on the simulation result we demonstrate that our IDS can mitigate significantly black hole attacks and secure the routing processes. The results show that proposed IDS reduces the impact of black hole attack (*simple and malicious*) to only 2 percent. Indeed, the black hole node is selected as a CH only one time, and immediately detected and excluded at next transmission phases. Which explain the lost of 2% of messages.

4.2.2 Selecting forwarding attack

The proposed IDS can also deal with selecting forwarding attacks which represent a particular type of black hole attacks. Figure 5 shows the obtained results.

4.2.3 Energy efficiency

The last experimental simulation consists of evaluating the amount of energy consumed by our IDS.

As shown in Figure 6, proposed IDS consumes negligible additional power for implementing intrusion detection based on security solution. Also, it is extremely energy-efficient as compared to conventional sensor node based system. Indeed, our IDS consumes 17 joules to detect 10 intruder nodes which represent 4.8 % of the overall network consumption.

5. Conclusion

We proposed an energy efficient intrusion detection system, to secure network nodes from black hole attacks. Our approach is simple and based on the exchange of control packets between sensor node and base station. Therefore, BS takes the role of monitor node to detect any black hole attack. We don't claim that the proposed mechanism can prevent definitively all black hole attacks; however our proposal mitigates significantly the impact of the attacks. Simulation results show the performance provided by our IDS in terms of security and energy saving. As future work, we will compare the performance of our security scheme with other black hole security mechanisms.

References

[1] Heinzelman, W. R., Chandrakasan, A., Balakrishnan, H. (2002). An Application-Specific Protocol Architecture for Wireless Micro sensor Networks, *IEEE Transactions on the wireless Communications*, 1 (4) 660-670.

[2] Lindsey, S., Raghavendra, C. (2002). PEGASIS: Power-Efficient Gathering in Sensor Information Systems, *IEEE Aerospace Conference Proceedings*, 3 (9-16) 1125-1130.

[3] Manjeshwar, A., Agrawal, D. P. (2002). TEEN: A routing protocol for enhanced efficiency in wireless sensor networks, *In*: 2nd International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing (WPIM), p. 195b.

[4] Boubiche, D., Bilami, A. (2011). HEEP (Hybrid Energy Efficiency Protocol) Based on Chain Clustering, *Int. J. Sensor Networks*, 10 (1/2) 25 - 35.

[5] Karlof, C., Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures, *In*: Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, p. 113-127, May.

[6] Newsome, J., Shi, E., Song, D., Perrig, A. (2004). The Sybil attack in sensor networks: Analysis and defenses, *In*: Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, p. 259-268,ACM Press.

[7] Deng, H., Li, W., Agrawal, D. P. (2004). Routing Security in Wireless Ad Hoc Networks, *IEEE Communications Magazine*, 40 (10), October .

[8] Krontiris, I., Dimitriou, T., Freiling, F. C. (2007). Towards intrusion detection in wireless sensor networks, *In*: Proceeding of the 13th European Wireless Conference, (EW' 07), CiteSeer.

[9] Lou, W., Kwon, Y. (2006). H-SPREAD, A hybrid multipath scheme for secure and reliable data collection in wireless sensor networks, *IEEE Transactions on Vehicular Technology*, 55 (4) 1320–1330.

[10] Jian, Y. (2006). A hierarchical secure routing protocol against black hole attacks in sensor networks, *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, V.1.

[11] Karakehayov, Z. (2005). Using REWARD to detect team black-hole attacks in wireless sensor networks. *In*: ACM Workshop on Real-World Wireless Sensor Networks.

[12] Satyajayant, M., Kabi, B., Guoliang, X. (2011). BAMBi: Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks, *IEEE ICC proceedings*.