ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 2, Issue 2, pp: (135-139), Month: October 2015 – March 2016, Available at: www.paperpublications.org

An Energy Efficient Scheme against Power Exhausting Attacks in Wireless Sensor Networks

[1]J.Joel Jino Moses, [2]V.Bibin Chirstopher

[1]P.G student,[2]Assistant Professor, Department of Computer Science Ponjesly College of Engineering, Nagercoil

Abstract: **A wireless sensor network (WSN) is an technology playing a vital role nowdays. One of the major challenges wireless sensor networks face today is security. Security and energy efficiency are critical concerns in wireless sensor network (WSN) design. The power of wireless sensor networks lies in the ability to deploy large numbers of tiny nodes that assemble and configure themselves. The denial of service attack,which tries to keep the sensor nodes awake to consume more energy of the constrained power supply.An anti-node can send fake data packets to sensor node of unprotected wireless sensor network to initiate unnecessary transmission repeatedly.This consumes more energy and reduces lifetime of sensor nodes.Using cross layer design the energy consumption is reduced. This paper aims with power exhausting attacks and energy consumption on wireless sensor networks.**

Keywords: **Wireless sensor networks, security, power exhausting, energy efficiency, cross layer design.**

1. INTRODUCTION

The emerging field of wireless sensor networks combines sensing, computation, and communication into a single tiny device. Sensor networks are primarily designed for real-time collection and analysis of low level data in hostile environments. The WSN is built of nodes from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors.The denial of service attack,which tries to keep the sensor nodes awake to consume more energy of the constrained power supply.An anti-node can send fake data packets to sensor node of unprotected wireless sensor network to initiate unnecessary transmission repeatedly.This consumes more energy and reduces lifetime of sensor nodes.Using cross layer design the energy consumption is reduced and also the lifetime is increased.

2. ATTACKS IN WIRELESS SENSOR NETWORKS

Attacks against wireless sensor networks could be broadly considered from two different levels of views.

- The attack against the security mechanisms.
- Against the basic mechanisms.

2.1 Denial of service:

The Denial-of-Sleep is one of the power exhausting attacks of WSNs. This attack is a special type of Denial-of-Service (DoS) attack, which tries to keep the sensor nodes awake to consume more energy of the constrained power supply. An anti-node can send fake data packets to sensor node of unprotected WSNs to initiate unnecessary transmissions repeatedly. It causes the jamming of a node or set of nodes. The jamming of a network can come in two forms: constant jamming, and intermittent jamming. Constant jamming involves the complete jamming of the entire network. No messages are able to be sent or received. If the jamming is only intermittent, then nodes are able to exchange messages periodically, but not consistently.

3. POWER EXHAUSTING ATTACKS

The denial of sleep attack is one of the power exhausting attacks in wireless sensor network[1][3],[7][9].This attack is a special type of denial of service attack,which tries to keep the sensor nodes awake to consume more energy of the constrained power supply.An anti-node can send fake data packets to sensor node of unprotected wireless sensor network to initiate unnecessary transmission repeatedly**.**

Without security mechanism,anti node can broadcast a fake preamble frequently in the sender initiated schemes.It the receiver cannot tell the real preamble and the fake one,the receiver will receive and process the data from the anti-node.Such attack will keep the receiver awake as long as the data transmission sustains,which exhausts the battery of node rapidly.Moreover,an anti-node can reply a fake preamble ACK to the sender.Thus,the sender will start to send data to the anti-node but it will never receive the right data ACK.Similarly,the sender may send data repeatedly and exhaust the battery of node rapidly.In receiver-initiated schemes,an anti-node can broadcast a “fake beacon” to cheat sender to process and send the data to the anti-node but it will never receive the right data ACK.An anti-node can reply a fake beacon ACK to the receiver.Thus,the receiver will never receive and process the data from the anti-node.

3.1 EXISTING SYSTEM:

3.1.1 B-MAC:

The B-MAC is an LPL based WSN MAC protocol[4], which decouples the sender and receiver with time synchronization.The receiver wakes up periodically to sense the preamble from the sender and then to receive and process the data.When the sender needs to send data,it sends a long preamble to cover the sleep period to ensure the receiver waking up and sensing.Figure 1 shows the process done in B-MAC protocol.

The B-MAC protocol has no ACKs and the receiver has to listen and to wait for the long preamble sended from the sender.This long preamble design of LPL based protocol consumes the major energy of both sender and receiver.Existing method insufficient to protect the WSNs from denial of sleep attacks in MAC layer.

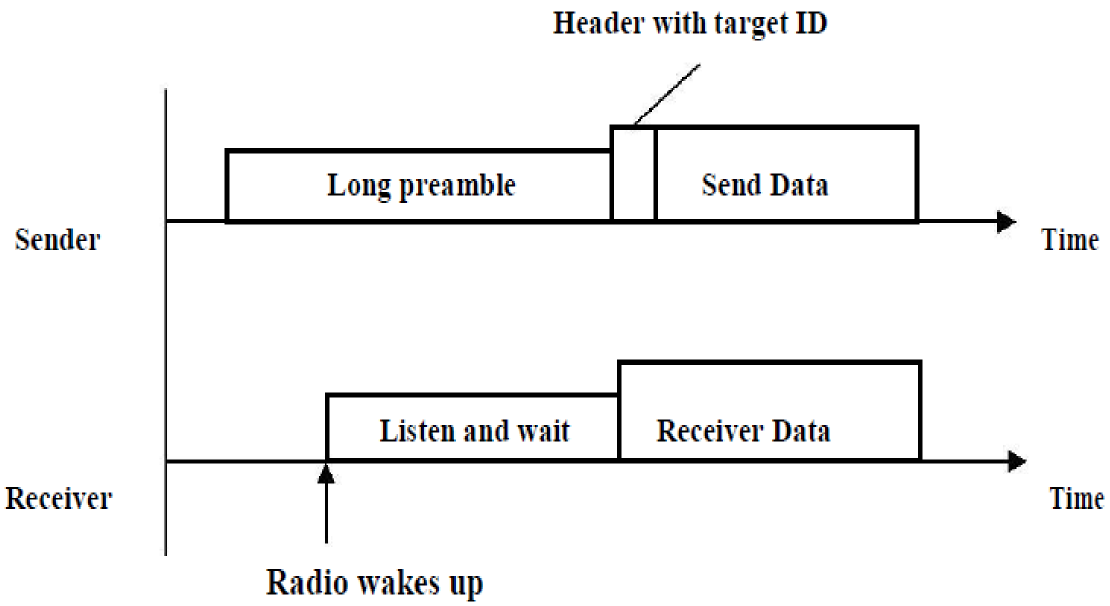

Figure 1: Timeline of B-MAC protocol

3.2 PROPOSED SYSTEM:

3.2.1 X-MAC:

A cross-layer design of secure scheme integrating the MAC protocol is used.Two-Tier Energy-Efficient Secure Scheme (TE2S) is proposed to protect the WSNs from the existing attacks based on our preliminary frameworks[5][6].This cross-layer design involves coupling two layers at design time without creating new interface for information sharing at runtime[8].This project proposes a two-tier secure transmission scheme. This scheme uses the hash- chain to generate the dynamic session key, which can be used for mutual authentication and the symmetric encryption key. The only computations of dynamic session key are the hash functions SHA-1, which is very simple and fast.By integrating with MAC protocol, there is no extra packet compared with the existing MAC designs.The two-tier design can check and interrupt the attacks at different check points. The combination of low complexity security process and multiple check points design can defense against attacks and send the sensor nodes back to sleep mode as soon as possible.Figure 2 shows the timeline of X-MAC protocol.

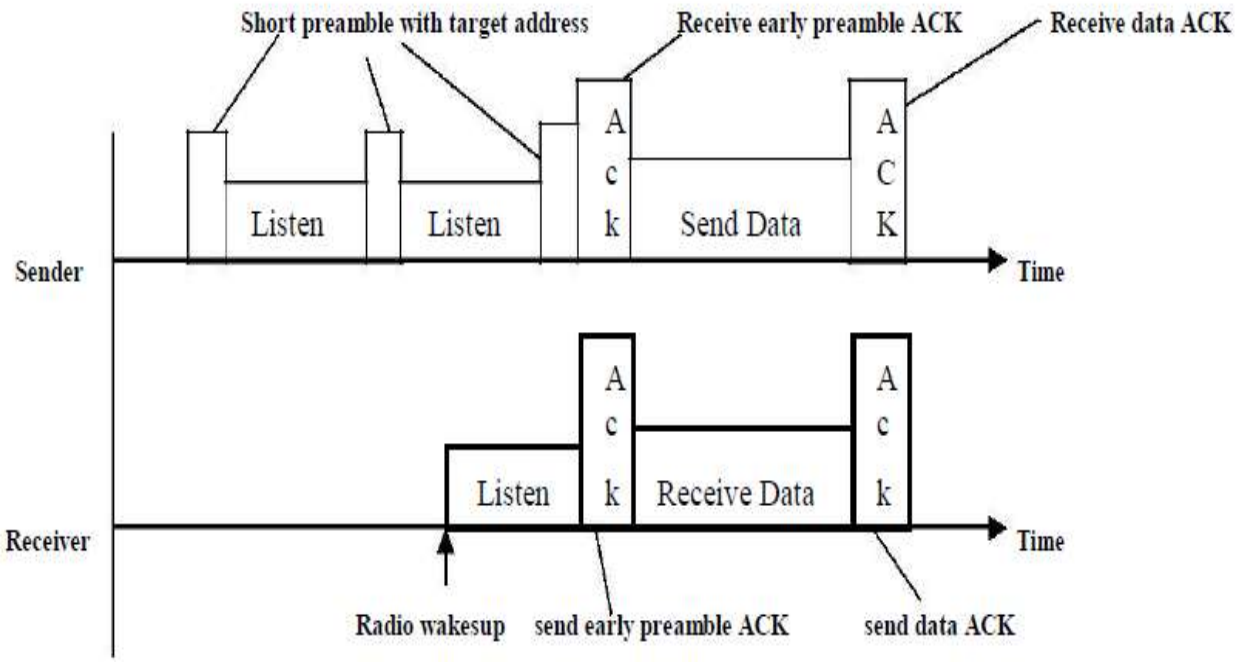

Figure 2: Timeline of X-MAC protocol

X-MAC protocol improves LPL based B-MAC protocol by replacing the long preamble with short preambles.The above fig shows the timeline of X-MAC protocol,which allows the receiver to send ACK back to the sender as soon as it senses the preamble.This short preamble design reduces the energy consumption of both the sender and receiver.

3.3 TE$_2$S:

The basic goal of the proposed model is to reduce the energy that is exhausted from the node. This can be overcome by applying clustering method and key generation method to the node. This can be performed by detecting antinode to transmit the data. To detect the anti-node the node wants to broadcast a hello message to the neighboring node.

The neighboring node response with the correct key that is already provided means the neighboring node with the correct response form a cluster. If not means that one is mark as an anti-node and detected. And to select the cluster head the node which has a maximum response it is marked as a cluster head. And then cluster gateway is selected thus the cluster member and the cluster head is selected. Then the key distribution phase is used to transmit the data at each node. The key is formed with the help of hash function. If the key is valid means the cluster member turn into a-wake state if not means it go back to the sleep state. Thus the power exhausting attack is considerably reduced and also energy consumption is reduced.

3.4 SYSTEM ARCHITECTURE:

The energy efficient architecture for power exhausting attacks is given in the figure 3.The basic goal of the proposed model is to reduce the energy that is exhausted from the node. This can be overcome by applying clustering method and key generation method to the node. This can be performed by detecting antinode to transmit the data. To detect the anti-node the node wants to broadcast a hello message to the neighboring node.

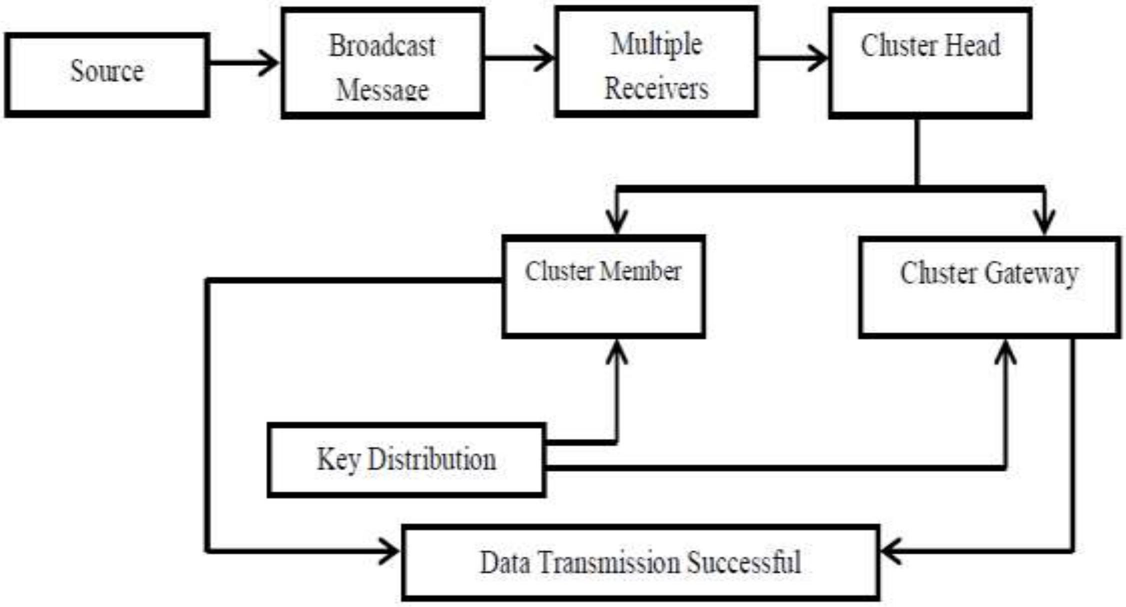

Figure 3: Architecture for Energy Efficient Scheme against power exhausting attacks

The neighboring node response with the correct key that is already provided means the neighboring node with the correct response form a cluster. If not means that one is mark as an anti-node and detected. And to select the cluster head the node which has a maximum response it is marked as a cluster head.

And then cluster gateway is selected thus the cluster member and the cluster head is selected. Then the key distribution phase is used to transmit the data at each node. The key is formed with the help of hash function. If the key is valid means the cluster member turn into a-wake state if not means it go back to the sleep state. Thus the power exhausting attack is considerably reduced. The source node broadcast the hello message to its neighbor nodes. The distributed key is passed to all sensor nodes. The nodes which are not able to decrypt the message will be the anti-node.

The nodes are grouped as the clusters. The cluster formation is done by the received hello messages. The node which receives more acknowledged hello will be the cluster head and remaining are the cluster members. The communication between two cluster are done by the cluster gateway. Now the key is distributed with in the cluster for data transmission process. Once the key is distributed the nodes access the data using the decryption process.

4. DESIGN PRINCIPLES OF TE$_2$S

The proposed cross-layer design, Two-Tier Energy-Efficient secure Scheme integrates the MAC protocol and involves coupling two layers without creating new interface for information sharing at runtime ,which aims to protect the WSNs from Denial-of-Sleep attack.

4.1 Sender-Initiated Scheme:

Step1: The sender selects random number Rs and computes the secure token (i.e.Token=h(kc|Rs),where h(x) denotes a one-way hash function with input x and the vertical bar | denotes concatenation of strings.

Step 2: The sender sends its ID (IDs*)*, receiver's ID (IDr*)*,secure token and random number Rs as the preamble.

Step 3: The receiver verifies the secure token. If the token is not valid, the receiver goes back to sleep mode immediately. If the token is valid, then receiver selects a random number Rr and computes the session key Ks = *h*(Kc|Rs|Rr*)*. The receiver also computes the hash chain *h*(Ks*)* and *h(h*(Ks*)).*

Step 4: The receiver sends the *h(h*(Ks*))* and random number Rr as the ACK.

Step 5: The sender computes the session key Ks = *h*(Kc|Rs|Rr*)* and the hash chain *h*(Ks*)* and *h(h*(Ks*))*. The sender then verifies the *h(h*(Ks*))*.If the *h(h*(Ks*))* is not valid, the sender will not send the data.

4.2 Data Transmission:

Step 1: The sender sends the *h*(Ks*)* and EKs(DATA | MACKs(DATA)) to receiver. The EKs(x) denotes encrypts x by using symmetric algorithm with key Ks. The MACKs(DATA) denotes the message authentication function with key Ks, where DATA is the input message.

Step 2: The receiver verifies the *h*(Ks*)*. If the *h*(Ks*)* is not valid, the receiver goes back to sleep mode immediately. If the *h*(Ks*)* is valid, the receiver decrypts the data and checks the MAC of data.

Step 3: The receiver sends the data ACK to sender**.**

5. TOTAL ENERGY CALCULATION

The total energy calculation is calculated using the formula as given below,

Consume energy=initialenergy-finalenergy

The initial energy is the energy which is at the starting of the process,and final energy is the energy produced at the final stage.By subtracting the initial and the final energy total energy consumption value will be achieved

6. CONCLUSION

The practical design is to simplify the authenticating process in order to reduce the energy consumption of sensor nodes and enhance the performance of the MAC protocol in countering the power exhausting attacks. A cross-layer design of secure scheme integrating the MAC protocol analyses show that the proposed scheme can counter the attack in an energy-efficient way.The Energy consumption is reduced using the proposed method and also the lifetime of the sensor nodes are increased.

REFERENCES

[1] M. Brownfield, Y. Gupta, and N. Davis, “Wireless sensor network denial of sleep attack,” in Proc. 6th Annu. IEEE SMC Inf. Assurance Workshop (IAW), New York, NY, USA, Jun. 2005, pp. 356–364.

[2] M. Buettner, G. V. Yee, E. Anderson, and R. Han, “X-MAC: A short preamble MAC protocol for duty-cycled wireless sensor networks,” in Proc. 4th Int. Conf. Embedded Netw. Sensor Syst. (SenSys), Boulder, CO, USA, 2006, pp. 307–320.

[3] R. Falk and H.-J. Hof, “Fighting insomnia: A secure wake-up scheme for wireless sensor networks,” in Proc. 3rd Int. Conf. Emerg. Security Inf., Syst. Technol. (SECURWARE),

[4] W. Ye, J. Heidemann, and D. Estrin, “An energy-efficient MAC protocol for wireless sensor networks,” in Proc. 21st Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM), Los Angeles, CA, USA, 2002, vol. 3, pp. 1567–1576.

[5] C.-T. Hsueh, C.-Y. Wen, and Y.-C. Ouyang, “A secure scheme for power exhausting attacks in wireless sensor networks,” in Proc. 3rd Int. Conf. Ubiquitous Future Netw. (ICUFN), Dalian, China, Jun. 2011,pp. 258–263.

[6] C.-T. Hsueh, C.-Y. Wen, and Y.-C. Ouyang, “Two-tier receiver-initiated secure scheme for hierarchical wireless sensor networks,” in Proc. 12thInt. Conf. ITS Telecommun. (ITST), Taipei, Taiwan, 2012, pp. 254–258

[7] 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 Trans. Veh. Technol., vol. 58, no. 1, pp. 367–380, Jan. 2009.

[8] V. Srivastava and M. Motani, “Cross-layer design: A survey and the road ahead,”IEEE Commun. Mag., vol. 43, no. 12, pp. 112–119, Dec. 2005.

[9] F. Stajano and R. J. Anderson, “The resurrecting duckling: Security issues for ad-hoc wireless networks,” in Proc. 7th Int. Workshop Security Protocols, London, U.K., 1999, pp. 172–194.Athens, Greece, Jun. 2009, pp. 191–196.