International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 04 | Apr -2017 www.irjet.net p-ISSN: 2395-0072

Energy Efficient Secure Scheme for Wireless Sensor Networks

Abhilasha K M, Shwetha V, Ashritha Kumari K S, Sindhu T R, Rekha K S

Dept. of Computer Science and Engineering, The National Institute of Engineering, Mysuru Karnataka, India

---

Abstract - *The major issues in Wireless Sensor network design are security and energy efficiency. This paper aims to develop an energy-efficient secure scheme against power exhausting attacks, especially denial-of-sleep attack, due to this denial of sleep attack WSNs lifetime will be shortened. Several MAC protocols have been proposed to save power and extend the lifetime of WSNs but these protocols are insufficient to protect nodes from denial of sleep attack. The existing known security mechanism awakes the sensor nodes before it undergoes security processes which take long duration to authenticate which is vulnerable to denial of sleep attacks. Therefore this design is concerned on simplifying the authentication process to reduce energy consumption of sensor nodes and increases the performance and also it eliminates forge attacks and replay attacks.*

***Key Words*: wireless sensor network, energy efficiency, denial-of-sleep, power exhausting attacks, secure scheme.**

1. INTRODUCTION

A wireless sensor networks mainly consists of base station and sensor nodes. The base station sends a broad cast message to all sensor nodes to form a cluster and select the head node. The other sensor nodes in a cluster do not directly interact with the base station. The interaction between the sensor nodes and base station is via head node. This is shown in the fig-1. It helps in best utilization of battery. If each sensor nodes send data to base station it consume all sensor node battery instead the sensor nodes sends a data to near head node and the head forward the data of all sensor nodes in the cluster along with its own data to base station.

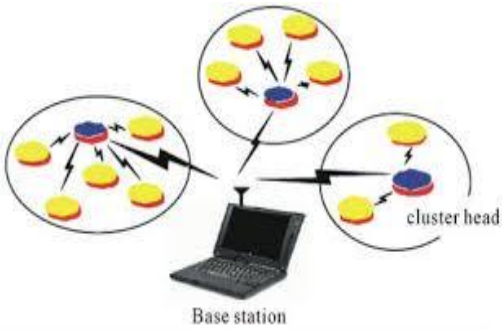

Fig-1 wireless sensor networks

In the above fig-1 the security and energy efficiency are the critical concerns. Various MAC protocols have been proposed to overcome this problem but these are not efficient for WSNs design [1-4]. WSNs are vulnerable to malicious attack whose target is sensor node power supply which results in denial of sleep attack. This type of attack reduces sensor life time from years to days [5].

X-MAC protocol is a low power protocol for a WSNs. X-MAC approach is simple and asynchronous. It has long preamble which results in excess latency at each hop and also suffers from excess energy consumption at non target receivers [6]. In ordered to reduce the inefficiency of X-MAC and also B-MAC we are using RI-MAC protocol. RI-MAC is a receiver initiated protocol in this first the receiver sends beacon message to the sender to inform that it is ready to receive the data then if sender has any data to send it sends the acknowledgement, after that it sends data to the receiver. Otherwise it does not send the acknowledgement [7].

2. LITERATURE SURVEY

In [6], M. Buettner, G.V Yee, E. Anderson, and R.Han. This paper presents X-MAC, a low power MAC protocol for Wireless sensors networks (WSNs). Standard MAC which is default MAC protocol for tiny operating system employ an extended preamble. Long preamble introduces excess latency and results in low power communication. X-MAC developed shortened preamble to minimize low power communication. These existing designs of MAC protocol are insufficient. The issues of this protocol can be overcome by using RI-MAC protocol which is a receiver initiated protocol and it will be used in our project.

In [5], D. R. Raymond, R.C. Marchany, M.I. Brownfield, and S. F. Midkiff. This paper presents in Wireless Sensor Networks the major issue found is Denial-of-Sleep attacks. In this paper they have used several MAC layers protocols for authenticating process. In present system when the sensor nodes sense the data, they encrypt their data and send it to the head node. To check the whether the node is authorized or not the head node had to decrypt that message and see it is from authorized node or not. This process takes long duration and consumes a head node battery life. To overcome this in our paper we simplified the authentication process by adding MAC code. The sensor nodes send an encrypted message to the head along with MAC code. To check the node is authorized or not head node verifies the MAC code and no need to decrypt the message. This saves the battery life of head node.

3. EXISTING SYSTEM

The authentication process in the present system for verifying the malicious node is lengthy and time consuming. The data send by the sensor node is encrypted using the cluster key. To verify the malicious node, head node has to undergo complete decryption process. Due to this complete decryption process it also shorten the battery life of head node and this leads to the early death of head node. After the death of the head node it has to carry out the process again for new head node selection this also consume battery life of all sensor nodes and time.

4. PROPOSED SYSTEM

In our paper we simplified the authentication process by adding MAC code. The sensor nodes send an encrypted message to the head along with MAC code. To check the node is authorized or not head node verifies the MAC code if the MAC code is valid then only it undergo decryption process otherwise no need to decrypt the message. This reduces the power consumption in WSNs. Our paper also defense against replay attack and forges attack.

In our paper implemented the cluster formation, key distribution and key renewal modules. The data requisition, message authentication and message forwarding modules are yet to be implemented.

5. METHADOLOGY

5.1 .Cluster formation

There are many sensors are randomly distributed in WSNs. This module shows how the neighboring sensor nodes form a cluster. In this system there is one base station, one head node per each cluster, and many sensor nodes. The all authorized sensor nodes are already had pre-distributed keys.

Each sensor node in a WSNs are send a encrypted "HELLO" to the neighboring nodes and this message is alive up to some milliseconds so the sensor nodes which are far away from the node can't receive this message, only nearest sensor nodes can receive. This is done by using the "Authenticated Broadcasting Mechanism (hello encrypted pre distributed keys).

After each sensor nodes are finished the exchange of "HELLO" message if they are authorized nodes then it states passed, after some time they replied to the one another by sending the count that is number of "HELLO" messages they received. If any malicious node sends any message to the sensor node then it showed as failed in red color, because it does not send the message which is encrypted with the pre-distributed key.

After exchange of count each sensor node compares the count with their count if its count is greater than the others then it is declared has head node. This head node send the IP address of the all sensor nodes which sends the "HELLO" message to this node along with its IP address to the base station and registered as a cluster. This is done by using "Adaptive Distributive Topology Control Algorithm (ADTCA), if the two nodes are eligible to be a head node the node which is registered first is considered as a head. For encryption we use a rijindal algorithm.

5.2 Key distribution and key renewal

After the head node registered its cluster in the base station the head node get a unique cluster id. The base station sends a cluster key which is encrypted with the pre-distributive key to the head node. The head node then distributes that cluster key encrypted with pre-distributed key to all the sensor nodes in the cluster. The unauthorized sensor node can't get the cluster key because it does not have a pre-distributed key.

The unauthorized sensor nodes may have chances of getting a cluster key. To avoid this situation after some particular time the base station renewal that key.

5.3 Data requisition

The sensor nodes in the cluster if they sense any data they must send their data to the head node when head is awake. The head node collects the data of all sensor nodes in the cluster and sends it to the base station along with its own data. If any emergency they can send their data to the head node at any time.

The energy efficiency is the one of the critical concern in WSNs. The head and sensor nodes are goes to sleep for some time and then awake for some time. This will increase the battery life of sensor nodes. We use the RI-MAC protocol.

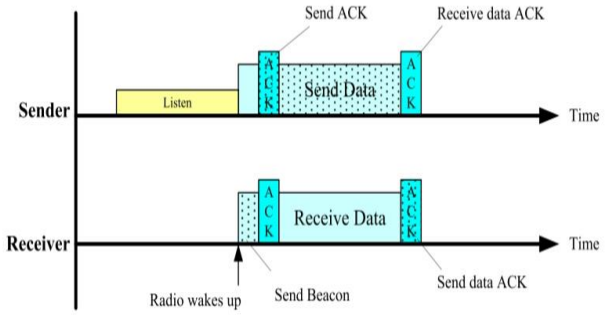

Fig-2 Timeline of RI-MAC protocol.

This Fig-2 represents the RI-MAC protocol in that when the head is awake it sends a beacon to the all sensor nodes in cluster that shows the head is ready to receive the

data from sensor nodes. Then the sensor nodes are sends their data to the head node this will save the energy.

5.4 Message authentication and forwarding

When the sensor nodes in WSNs senses the data, they encrypt their data using the cluster key and generate MAC code using hashing algorithm and send the encrypted data to the head node along with the MAC code. The head node receives the encrypted data and MAC code and it verify MAC code to check whether the sensor nodes are authorized or not. If the sensor node is authorized then only the head node is decrypt the message and check the message is valid or not. If the message is valid then it sends that data to the base station by encrypting.

If the any unauthorized node sends the data to the head node it verifies the MAC code. When the verification failed it does not goes for decryption and it discard that message. The authentication process simplified here hence it saves energy.

6. IMPLEMENTATION

The implementation includes creation of base station, creation of sensor nodes, and creation of cluster and head registration.

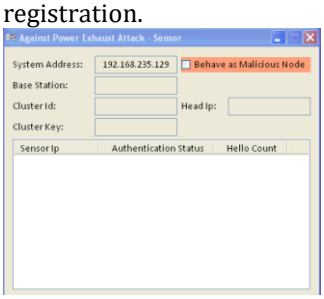

Fig-3. Sensor node

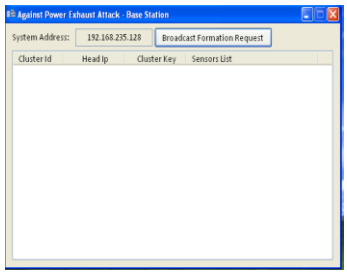

Fig-4. Base station

The above Fig-3 represents the sensor node, it consists of its own IP address in the beginning and after the cluster is formed it has the details like, base station IP address, cluster id, cluster key, and head node IP address. It also consists of the other sensor IP address list (sensor IP) that exchanges the message with these if they are authorized then authentication status is passed if they are malicious nodes then authentication status is failed. They also exchange the number of "HELLO" they received (Hello count).The sensor node can be act as malicious node if we selected behave as malicious node field in the sensor.

The above Fig-4 represents the base station. It consists of its own IP address and if we click on broadcast formation request field then it tells all the sensor node form a clusters. It also have the following fields after the clusters are formed, cluster id is generated using the IP address of all sensor node in the cluster, header IP consists of IP address of the head of the cluster, the cluster key given for data exchange unique to each clusters and sensors list is IP address of all sensor nodes in the cluster.

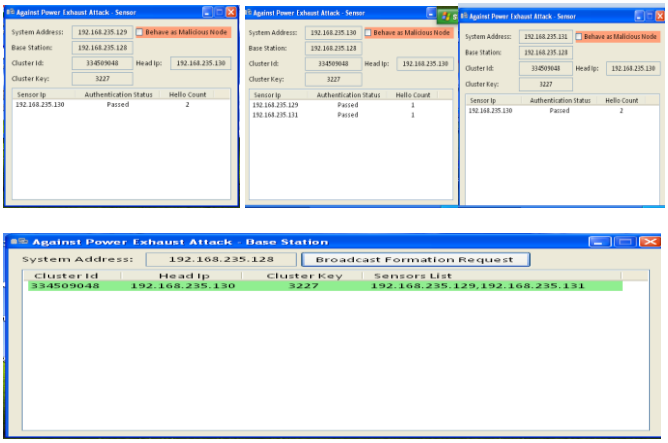

Fig-5 cluster formation and key distribution

In the above Fig-5 we represent cluster formation using three sensor nodes. Considered three sensor nodes each can ping to remaining two, but we blocked the exchange of message between the first and the last using IP Blocker in the first and last node. So they can't exchange the message.

When the base station click on the broadcast formation request it sends the cluster formation request message to all sensor nodes using UDP protocol. When sensor nodes received this message they start exchanging "hello". The middle sensor node exchange the "hello" with remaining two but the first and last exchange "hello" with only middle one. All three sensor nodes are authorized because they exchanged the "hello" which is encrypted with pre distributed key so the authentication status is passed.

After they exchanged the "hello" message they exchange the count. Then each sensor node compares their count with the count they received. If their count is grater then they registered as head. The middle sensor node count is two the others count is one so the middle sensor node registered as head in base station as shown in Fig-4.

when the middle node is registered as head with unique cluster id, The cluster id is created by using all sensor node IP addresses by sorting IP addresses of sensor nodes and then a hash code is generated which is referred as cluster id. The head IP fields in sensor nodes are filled with middle node IP address and also cluster id and cluster key fields are filled.

The sensor node can act as a malicious node if we select behave as malicious node field. Now consider the three sensor nodes and one base station.

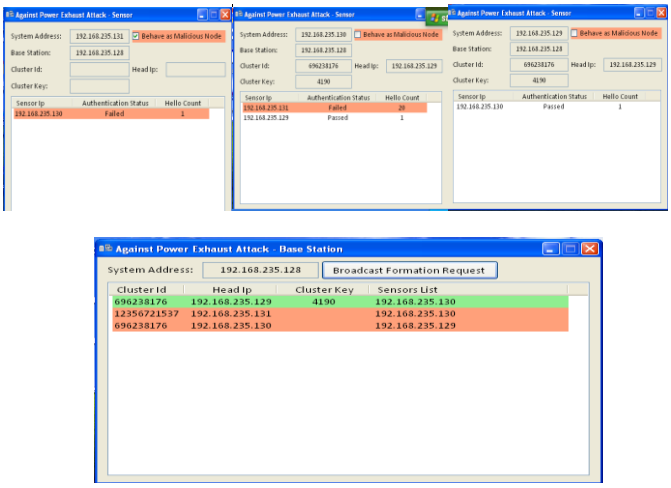

Fig-6 Act of malicious node

Above fig-6 represents the first node is act as malicious node and remaining two are authorized nodes. When base station send the cluster formation request to all sensor nodes this malicious node is also exchanges the "hello" but it is not encrypted using the pre-distributed key hence the authentication status is failed and displayed in red color. Second and the third node exchange the "hello" and the count. But both nodes count is one and both are eligible to become a head but the node which is registered first becomes the head. In the above figure-5 the second node registered earlier than the third one so the second one becomes the head. The malicious node is also generate some random cluster id and try to registered as head but the cluster id generated by the malicious node does not follow the authorized cluster id generation technique so the base station get to know that is a malicious node and does not considered its registration.

7. FUTURE ENHANCEMENT

This paper uses an ADTCA algorithm for selection of head in the cluster. This selects the head based on which sensor node has a high number of "HELLO" counts, that is which node is near to all sensor node in the cluster is selected has a head. This will increase the life time of sensor nodes.

This algorithm does not consider the other resources like their battery life. This algorithm selects the middle node in the cluster has head but does not consider the battery life it can be dead soon compared to other nodes in the cluster. If the head node is dead then we need to elect other node as head, this consumes more energy.

Another algorithm called HEF (high energy first) it selects the head based on the node in the sensor which has highest battery life. But it can be far away from the other sensor nodes in the cluster. To send the data from sensor nodes to the head node it consumes more energy of sensor nodes. This is not efficient algorithm.

In future, need to implement the algorithm that selects the head based on their resources and the number of counts they exchanged. This will save the energy of sensor nodes.

8. CONCLUSION

This paper proposes a cross layer design of energy efficient secure scheme. This simplifies the authentication process and reduces the power consumption in sensor nodes. Due to the simplified authentication process and multiple check points, this design defense against denial of sleep attack, forge attack, and replay attack.

This scheme is efficient in both sender initiated scheme and receiver initiated scheme. This also extends the life time of WSNs under attack. The overall concept is to extend the battery life of the sensor nodes.

REFERENCES

[1] G. P. Halkes, T. van Dam, and K. G. Langendoen, "Comparing energy saving MAC protocols for wireless sensor networks," *Mobile Netw.Appl.*, vol. 10, no. 5, pp. 783–791, 2005.

[2] A. Bachir, M. Dohler, T. Watteyne, and K. K. Leung, "MAC essentials for wireless sensor networks," *IEEE Commun. Surv. Tuts.*, vol. 12, no. 2,pp. 222–248, Second Quarter 2010.

[3] J. Kabara and M. Calle, "MAC protocols used by wireless sensor networks and a general method of performance evaluation," *Int. J.Distrib. Sensor Netw.*, vol. 2012, pp. 1–11, 2012, Art. ID 834784.

[4] Ching-Tsung Hsueh, Chih-Yu Wen and Yen-Chieh Ouyang "A Secure Scheme for Power Exhausting Attacks in Wireless Sensor Networks" Department of Electrical Engineering & Graduate Institute of Communication Engineering National Chung Hsing University.

[5] 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.

[6] 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.

[7] Y. Sun, O. Gurewitz, and D. B. Johnson, "RI-MAC: A receiver-initiated asynchronous duty cycle MAC protocol for dynamic traffic loads in wireless sensor networks," in *Proc. 6th ACM Conf. Embedded Netw.Sensor Syst. (SenSys)*, Raleigh, NC, USA, 2008, pp. 1–14.