ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Providing Security Against Attacks & Efficient Data Aggregation by Selection of Uncompromised Leader in WSN

[I]Sonali Joyce Lobo, [II]Dr. H.D Phaneendra
[I]PG Student, CNE, [II]Professor
[I,II]Dept. of IS&E, The National Institute of Engineering, Mysore, India

Abstract
Important Concerns of Wireless sensor networks(WSN) are Energy efficiency and security. The paper mainly pays an attention on increasing the lifetime of WSN. This can be achieved by solving variety of attacks. Stronger security and, higher network efficiency can be obtained by avoiding many kinds of attacks. This paper proposes a methodology of preventing various attacks such as Denial of sleep attacks(DOSLA), Replay attack, Forge attack. This paper also utilizes stature based framework of trust for the efficient selection of the cluster head. It also aims at reducing the power exhaustion by preventing DOSLA.

Keywords
Wireless Sensor Networks, Power Consumption, Energy Efficiency, Replay Attack, Forge Attack

I. Introduction

Computer Network (CN) is a grouping of devices which are interconnected with an aim of resource sharing. The most familiar shared resource is internet. Internet(INT) is accepted worldwide and is the main source of communication. A human in one country can communicate with the another using this source. It consists of interconnected CNs that communicate with IP suite. The common model used in INT is client-server model(CSM). CNs are divided into variety of topologies such as star, mesh, ring and, so on.

Wireless Sensor networks(WSN) contains device such as sensors which are distributed all over the network. Sensors obtain the information from the environment and directs it to the device called base station (BAST). BAST is a node which has more power than the other nodes. Its job is to collect the information and display it. Sensor nodes in WSN have very low power. Conservation of power is a critical issue. This issue must be handled in a proper manner. WSN consists of large number of nodes. If at all in such a network, a node sends the data to another one which is far out of reach, then the data might get lost. This problem should be avoided. Solution to this problem can be obtained by dividing this huge network into small groups. Then out of this group one will be selected as the head. The head performs the duty of collecting the data and forwarding to the gateway or, to the BAST. Such grouping is called a cluster and head is named as cluster head(CLHE). Member of the cluster other than CLHE are termed as Cluster members.

WSN faces lot of issues. Out of these one is security. There are many attacks which create many problems to WSN. These attacks can be categorized into two. First is the Active attack(AA). Second is the Passive Attack(PA). PA is accessing the information in an unauthorised manner. PA never tries modifying the data stolen. The main aim of the attack is stealing information and, understanding the pattern of it. In AA an attacker not only accesses information in an unauthorized manner but also modifies the data obtained by him. He might either use it for unintended purposes or, might delete the authorized data. AA is dangerous compared to that of the PA. This paper mainly places it focus avoiding AA in particular an attack named Denial of Service(DEOSA).

DEOSA - Denial to provide intended service. There are various kinds of DEOSA such as blackhole attack(BA), Denial of sleep attacks(DOSLA) & so on. In addition to attacks that are listed above the proposed model also tries solving replay attacks(RA) and forge attack(FA). In BA the node or device of the network drops the data or, withholds it, and, refuses to send it to the intended one. In RA attacker robs the data traversed and replays the data after sometime. In FA the attacker robs, modifies and, forwards the modified data to some other device of the network. In RA and FA, the intended node receives the invalid data.

The DOSLA causes Power Exhaustion(PE). This attack forces the nodes refuse to go to their rest state and in turn lose their power completely. This causes their death. The attacker is named as antinode (ANTN). This node frequently sends the invalid packets to some valid node of the network. If the valid node couldn't make out the sender as an invalid one, it will continuously process the data sent by it, by which it loses its power and, this leads to its death.

Further this paper is arranged as follows, first, the related works which describes the existing works related to the proposed model of this paper. Second, the concept of existing system. Third, the Proposed Model. Lastly, Conclusion and References.

II. Related Works

Ching-Tsung Hsueh, Chih-Yu Wen, Yen-Chieh Ouyang [1] have described a method to solve DOSLA in their paper. They have described two schemes sender- initiated scheme(SI) and receiver initiated scheme(RI). In the SI scheme ANTN enacts as a sender. In the RI scheme the receiver enacts as ANTN. In SI scheme ANTN continuously sends invalid preamble. If the receiver in SI scheme couldn't make out the sender to be an ANTN, it processes the preamble one after the another which leads to its death. The same way in RI scheme ANTN sends invalid beacon to which the valid sender sends the packet to it and thus leads to a case where the ANTN acquires valid packet and the valid sender never receives right beacon.

Wazid M, Katal A,Singh Sachan R, Goudar R.H, Singh D.P[2] described a method to detect and prevent BA. In this method firstly, a cluster is formed and also the sensors in the cluster are assigned an id. After forming a cluster, a coordinator is chosen. This coordinator will hold a table with the ids of the members of its cluster. Coordinator monitors and inspects the nodes to find a blackhole. If it finds a blackhole, removes that node from the cluster and reforms the cluster. This paper doesn't provide a mechanism to check the compromised CLHE in the network.

Anjali, Shikha, Sharma M [3] discussed variety of security hazards and challenges which the WSN has to face. The hazards discussed in the paper effects the WSN in a negative manner. The hazards

are flooding attack, Sybil attack, selective forwarding attack, wormhole attack and, so on. Flooding attack is a kind of DEOSA where in the attacker broadcast numerous invalid packets in the network, consumes resources and, thereby makes a service unavailable. It may also bring down the network service. Selective forwarding attack is slightly different from BA attack where in it doesn't drop all the packets but drops part of it.

The paper mentioned in the ref [4] describes about the LPL WSN MAC protocol so-called the B-MAC. In this protocol the sender forwards a long preamble. Periodically, the recipient awakes for sensing the preamble. Upon receiving the preamble, it performs further computations on the preamble. The LPL protocol utilizes substantial amount of energy of both sender and recipient.

The paper mentioned in the ref [5][6] proposes a wake up scheme. According to this sensor performs transition betwixt 2 states. The 2 states are Alive and Rest. Alive state is higher energy consumption state. Rest state is lower energy consumption state. The model mainly concentrates on solving sleep deprivation attack(SDA). This attack causes a node to always be in its alive state, makes it process the packets and ultimately makes it lose all its energy and die. This attack needs to be avoided. The solution mentioned in this paper solves it but, is not completely efficient compared to the proposed model. A more efficient hashing method is used in the proposed model. According to the existing model, when sensors go to the rest state, sensors configures Wake Up token(WAUT) ref values. These are stored in wake up radio. This radio waits for WAUT. Once the radio receives it, it verifies the token with the ref values it has. If the token matches, then only it wakes up the sensor.

II. Proposed System

The proposed model is valid only for single hierarchy network. The Topology formed is as such as described in the figure.

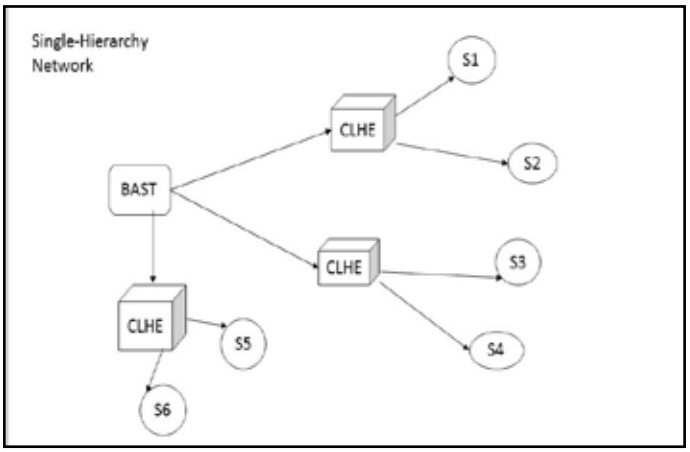

Fig. 1: Single Hierarchy Network

Figure 1 illustrates a single hierarchy network. It's a simple sample network with a single BAST with 3 CLHE and sensor nodes named S1, S2, S3, S4, S5, S6.

The proposed methodology involves solving both BA and DOSLA. These attacks are solved with the following objectives.

The first objective deals with **cluster formation**. This begins with BAST sending "request" to all the nodes in network. The nodes which receives the request, constructs a "Hello" packet and floods it to all the other nodes of the network. The nodes which sends the "Hello" also receives "Hello". In the first iteration the sensor node which receives the maximum count of hello's will become the CLHE.

The figure 2 depicts a single hierarchy network forming a single cluster and having a single CLHE. BAST represents the Base Station. S1, S2, S3, S4 are the sensor nodes. As S2 receives the highest no of "Hello's", it becomes the CLHE. Hello Packets are the beacon messages required for network formation.

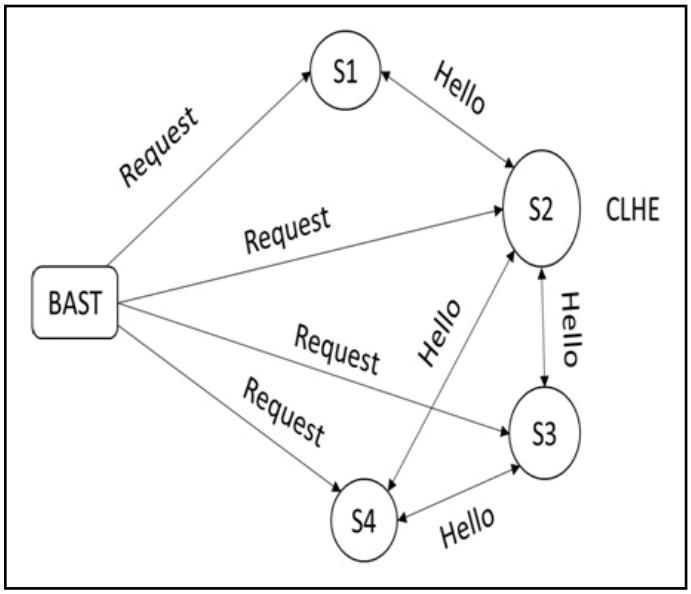

Fig. 2 : Procedure of Cluster Formation

The second objective deals with the **detection and, prevention of the ANTN** that causes DOSLA. This objective is carried as a part of the first objective and, is performed before the network formation. Before the transmission or, reception of the data, MAC code computation must be involved. Before the BAST broadcasts its request, it should calculate the MAC. The nodes before receiving the request it must validate the BAST by calculating MAC and Verifying MAC. The same way nodes before flooding their packets must calculate MAC. The Nodes before receiving the packets, they must calculate and, validate the sender by verifying MAC. Whenever the MAC matches the verification is successful, processing can be carried out. Otherwise nodes go to sleep, considering the sender to be an ANTN.

The main aim of clustering is to make the task of data aggregation easier. So the data aggregation must be carried out in a secure manner. Two methods used to carry out the secure data aggregation are encryption and decryption. Symmetric encryption and decryption methodologies are used. The data which the sensor sends is encrypted with the cluster key (CK). This objective deals with **CK distribution**. BAST encrypts the CK with its own specific key. After encryption of the key it unicasts the key to the CLHE. CLHE forwards it to other nodes of its cluster. Sensor nodes obtains the encrypted key from CLHE and, decrypts it. After decryption it obtains the CK. Using the same CK over and over may put the network into jeopardy. So CK must be renewed over each iteration. This objective also deals with the renewal process. This process is carried out by BAST generating a new CK.

The fourth objective is **Secure Data Aggregation** by BAST. The overall process carried out to attain this objective is as such, firstly Sensor nodes sense the data from the environment and, forwards the data to the CLHE. The CLHE collects the data from sensor nodes and unicasts it to the BAST as shown in the figure 3. The data transfer must be carried out securely. Thus before the data transmission and reception MAC is computed and verified.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

MAC verification is done to avoid the processing of data from the ANTN.

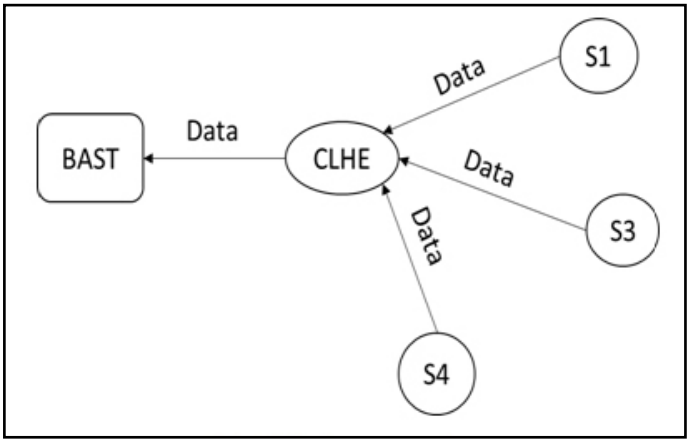

Fig. 3 : Data aggregation

The data collected by the CLHE must be forwarded to the BAST securely. This can only happen if the CLHE performs its responsibility correctly without getting compromised. If the CLHE gets compromised, it acts as a blackhole collecting the data but never forwarding to BAST. This black hole can either drop packets or never forward it to the intended node. The main aim of the fifth objective is to avoid such a blackhole from becoming a CLHE. This objective can be fulfilled by **trust management**. Trust value of the CLHE is calculated based on the drop limit. Drop limit is set to some value. If the CLHE drops the packet higher than the limit, such a node is prevented from becoming the CLHE.

IV. Conclusion

The proposed system of this paper achieves the reduction in power consumption by making use of hashing (MAC Code). It also avoids and prevents DOSLA, RA and, FA by making use of the same concept. By reducing the power exhaustion, proposed model increases the lifetime of WSN. The paper also tries increase the efficiency of data transfer by choosing a CLHE which is not under the influence of any BA.

References

[1] *Ching-Tsung Hsueh, Chih-Yu Wen, Yen-Chieh Ouyang, "A Secure Scheme Against Power Exhausting Attacks in Hierarchical Wireless Sensor Networks", Sensors Journal, IEEE, pp. 3590-3602, 2015.*

[2] *Wazid M, Katal A,Singh Sachan R, Goudar R.H, Singh D.P, " Detection and prevention mechanism for blackhole attack in Wireless sensor networks", 2013 international conference, communication and signal processing, pp.576-581, 2013.*

[3] *Anjali, Shikha, Sharma M, "Wireless Sensor Networks: Routing Protocols and Security Issues", Computing Communication and Networking Technologies (ICCCNT), 2014 International Conference, PP.1-5*

[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] *Rainer Falk, Hans-Joachim Hof, "Fighting Insomnia: A Secure Wake-up Scheme for Wireless Sensor Networks" 2009 Third International Conference on Emerging Security Information, Systems and Technologies, PP. 191-196*

[6] *Sonali Joyce Lobo, Sumana K.R, "Issues and Attacks -A Security Threat to WSN: An Analogy" Intenational Journal of emerging Engineering Research and Technology, ISSN online 2349-4409, Volume 4, Issue 1, pp. 96-99*