International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2017): 7.296

A Secure Method against Power Exhausting Attack in WSN

Jaya Kaushik[1], Dr. Naresh Grover[2]

[1]Department of ECE, Manav Rachna International University, Faridabad, Haryana

[2]Dean Academics, Manav Rachna International University, Faridabad, Haryana

Abstract: ***In the below presented work the DoS attack is being considered in the case of the wireless sensor network, which generally effects the battery backup for the connected devices. The DoS attacks consumes the necessary resources of the devices so as to make them unavailable at the time when needed. In the complete process the attack tries to reduce the energy efficiency of the network by consuming the extra energy and effects the energy structure management of the network. A novel method is being discussed so as to reduce the energy consumption of the devices in the WSN. The sensors used in the networks now a days are capable of detecting the factors like temperature, pressure, pollution, and many more other factors as per usage in the application field. The sensors which works for the detection of the low power mode generally makes the nodes to sleep mode so as increase the running life span of the devices. By analyzing existing C. T. Hsueh approach, prevention from DoS attack in WSN is proposed. The proposed methodology uses RSSI value with routing information to detect the malicious node and secure mechanism with cluster formation for further enhancement of this proposed approach are used in this work.***

Keywords: Wireless Sensor Network, Attacks, DoS, MAC, Classifiers, Bagging, Boosting, Meta Decision Tree, Data Mining, Ensemble, Errors, Learning, Training

1. Introduction

Wireless Sensor Networks (WSNs) are the self-configured network without any specific structure where it is able to carry out the natural and physical conditions like temperature, voice, vibrations, pressure, etc. and supposed to meant for passing on the information to the end generally termed as the sink, where it can be analysed and detected easily. The interface between the user and the network is termed as the sink of the network. Sink is the place where the user can go for their queries and also can get the answers in revert with respect to their query. A WSN is generally is a collection of number of sensor of nodes which can be like in hundreds or even in thousands.

Radio signal technique is being used for the communication between the sensor nodes inside the network. The main framing parts of any sensor nodes are like sensing unit, communication unit, radio transceivers and power management segment. There are number of other related features of any sensor node like the processing speed of the sensor nodes are limited, less storage, communication bandwidth available is quite less, etc. At the time when the sensor nodes are being deployed [1] in the network they are completely responsible for the infrastructure of the network means they can carry out the multi-hop kind of communication in the network. Right after the deployment of the sensor nodes the sensor which is onboard starts with the work of considering the data which is useful. The sensor nodes are also responsible for the queries from the "control site" for any response which might be related to the sensed information. The state of the sensing node can be defined in two forms as continuous or event driven.

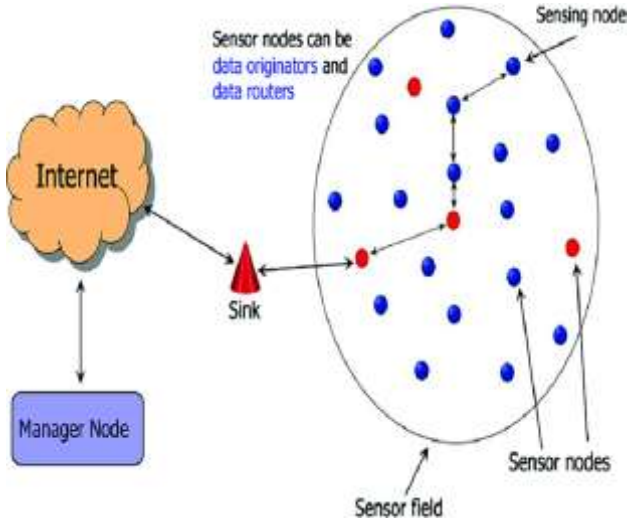

Figure 1: A typical Wireless Sensor Network

GPS (Global Positioning System) [2] and the local positioning system are two different techniques to get the positional information about the nodes on the network. Actuators are also sometime attached to the sensing nodes for properly taking action on the specific type of queries. Such type of the network are generally termed as the WSN or even Actuator Networks as per defined by (Akkaya et al., 2005) [3].

Just because of the special design issues the WSN requires some specific considerations or paradigm and also some new applications and usages are enabled by the category of the network. By considering the low power requirements and also should have the less complexity where the energy consumption also defines the life time of the nodes, there should be an effective balance between the capabilities of processing time and communication inside the network. The initial mentioned parts actually motivates the researchers in the research area of WSN which also includes like process

of standardization and also increased the investment in the research in previous years (Chiara et. al. 2009) [4].

2. Denial of Sleep

The nodes in the network which are generally sensing nodes are highly depended on the energy or power. For the case to keep the nodes in the continuous or working state for long it is necessary to maintain or manage the power consumption. For the conservation of the energy the nodes which are out of communication generally goes to sleep mode, the time and condition for the sleep mode are specifically defined. The attacks termed as Denial of Sleep attack are attacks which makes the radio to be awakened for most of the time just to exhaust the power of the sensing nodes. The Denial of Sleep attack are also termed as the Sleep deprival torture attack. The network can be disabled completely by both jamming and also by Denial-of-Sleep, as the jamming process takes quite more time to reach the state required and the slit decrease in the sleeping time will increase the power exhaust at large extent [5].

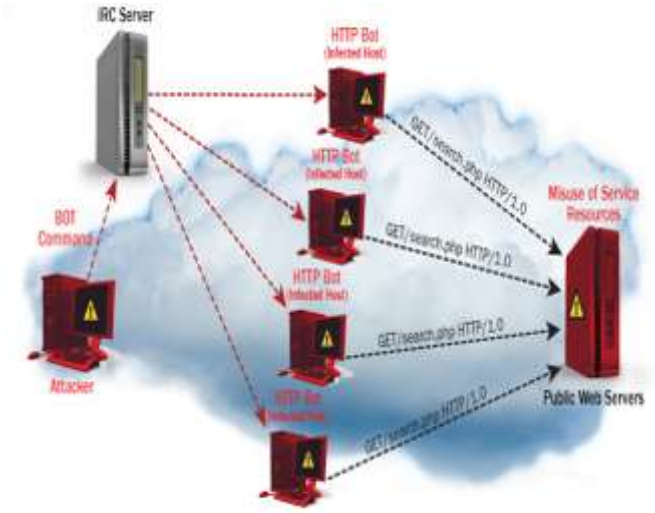

Figure 2: Denial of Sleep Attack.

3. Energy Consumption Issues In Wireless Sensor Network

As the sensor nodes are battery driven devices hence the consumption of the power is the critical factor for the sensing devices. The optimization of the consumption of the energy is considered as the major role-playing factor as it works for reducing the power consumption and alongside also works for increasing the life-span of the network. The optimization of the power consumption can be considered at the time design phase of the network and the sensor nodes and also at the time of considering the security factors. The awareness about the energy conservation is different for the sensor nodes and for the network as a whole as for the nodes it meant for the group of sensing nodes (Bharathidasan et al. 2001) [6].

Following are the four different sub-parts of the sensor node (Bharathidasan et al. 2001):

- **A computing subsystem:** The computing system inside the sensing device is generally termed as the microprocessor which is actually responsible for the activities like the control making between the nodes and also for the implementation of the communication protocols. MCUs generally considers various states for the purpose of power management. The different modes are generally being defined as like power consumption, level of power consumption, which are to be considered for going with the power consumption management for each and every node in the network.
- **a communication subsystem:** The sensor nodes are equipped with the radio communication facility and are capable for communicating with the neighbouring nodes means they have short range of communication. There are different working modes available for the radio. For the purpose of power optimization the radio device is supposed to be switched off in the case when they are not either sending or receiving any signal in the network.
- **a sensing subsystem:** It comprises of the number of sensors, actuators which actually provides the linking of the nodes and the communication devices with the network and the outside world more specifically we can consider the users as the outside world. The optimization of the power can be done by using the segments in the network or nodes which has low power consumption.
- **a power supply subsystem:** It is battery abled system which provides continuous power supply to the nodes. The consumption rate of the power for any nodes is needed to be checked because if high power passes to the node for long then the life-span of the network n and also nodes will be reduced, this part will make the battery to die early. The power generation by the battery is just more then the minimum requirement of power for any node to be running mode or for the transmission or to carry on the communication. The power consumption or the life-span of the node can be increased by reducing the power consumption or making the node in sleep state when it is out of transmission.

4. Related Work

This segment of the paper explains the related work on WSN which specifically talks about the security issues related to the power exhaustion.

In this work the author proposed a MAC protocol which considers many of the factors for the denial-of sleep attack which uses the centralized cluster management. Many features which deals with the energy saving are been considered by MAC which actually works for the energy saving and the centralized management makes it more prone to the denial of sleep attacks. A gateway node is being considered for the transmission of messages within the cluster or outside the cluster, the centralized structure also considers the two contention periods and also some different networks.

As per the performance analysis of the MAC protocol the G-MAC [7] performs efficiently than other protocols considering almost all traffic situations. The empty network case shows the protocol overhead and idle listening effects determined by the effective duty cycle-MAC has .95% duty cycle is weighted average of duty cycle of gateway node and other nodes. The gateway node can provide the access to the

attackers but in this case only single node will get affected as the responsibility of the gateway changes for nodes on the basis of battery level of the sensor nodes.

The DoS are categorized with respect to the information about the MAC layer that the attacker have and also with respect to the ability to bypass the encryption and authentication level of the network. A modelling is being done on four different MAC protocols as Sensor MAC (SMAC), Timeout MAC (T-MAC), Berkeley MAC (B-MAC), and Gateway MAC (G-MAC) [8]. Implementations of selected attacks on MAC, T-MAC, and B-MAC are described and analyzed in detail to validate their effectiveness and analyze their efficiency. As per the analysis it is quite clear that some attacks keeps the nodes awake upto 100% in the case when they are in sleep mode for 99% of there life spam, on S-MAC. In the case of the T-MAC the attacker can make the node ready to 100% as the node remains in sleep mode for 92percent of its life spam. As the data packets which are being transmitted over the network varies on the basis of the structure and also with respect to the time and with the knowledge of the structure of the protocols and the capability to bypass the encryption stage of the network because of which the networks are susceptible for the many types of attacks which actually results in the reduction of time of life time of the network and also maximizes the power consumption of the network.

Some attacks can be applied on the network without bypassing the encryption stage of the network for example subtle attack which reduces the life spam of the network when considering the magnitude order of the network. So as to meet the current requirements the network is supposed to face the problem of attacks and also the denial of sleep attack. Above described method increases the overhead of the network.

Raymond D. R. et al. [9] proposed a lightweight intrusion detection technique based on the host termed as Clustered Adaptive Rate Limiting (CARL), which on MAC layer of the protocol using the rate limiting technique and also works for opposing the DoS attacks. The major problem with the technique is about the synchronization of the awekening time of the node, as in the case when a node in the network sends data packet to the other node in the network then it is not sure that whether the node will consider the packet on time or what time the responding node will take to respond for the data packet. The latency in the case of the multi-hop network is being increased by B-MAC protocol, it considers the rate limiting process in the case when the access of traffic is available in the network and also sometimes results in the loss of the traffic of the network. So, in adaptive rate limiting, network traffic is restricted only when malicious packets have been sensed at a rate sufficient to suspect the attack.

Chen C. et al. [10] considered a method for the fake schedule with RSSI measurement aids. On the basis of the attacks in the past on the network the fake schedules are provided to the nodes in the network. By this method the chances of attacks on the network can be reduced as the network is having the proper schedule all the time and also the attackers may loose there power in attempting for the attack over and over again and may sometime go to dead condition. The health of the network is being considered or even assured when talking about the energy price and the delay of network, using the techniques reduces the packet drop ratio as compared to other techniques without having the fake schedules. Here in this paper we consider only S-MAC protocol with duty cycle 10%. The fake scheduling may harmful sometime in the case when there is no data packet loss. Due to which RSSI is used as a value assigned to each node and node having attacker one hop away has larger RSSI [11] value.

Tapalina Bhattasali et al. [12] a hierarchical framework is being presented along with the distributed collaborated mechanism so as to better detect the sleep deprivation torture in the case of the WSN. The nodes in the case of the heterogenous field are divided with respect to there roles in the network like sink gateway (SG), sector monitor(SM), Sector-in –charge (SIC) and leaf node (LN), on the basis of their power limit. The data is being sensed by the leaf node, data collection is being done the SIC, data validation is being done by the SM. For accessing the other networks the Sink Gateway is used.

In the case when the intruder affects the leaf node the same cannot be detected by the nodes. As a result of which the node which is affected by the intruder attack may loose the power may die completely. Such type of process is to be done in authentic manner as it affects the transmission of data over the network.

5. Issues and Challenges

Different issues and challenges of the WSN are as under:

- Security
- Hidden Terminal Problem
- Expose Terminal Problem
- Selection of Transmission Rate
- Power Control
- Nodes Mobility
- Real Time Traffic Support
- Energy Balance

6. Objective of Research

The main objective of this work is to introduce a framework for to resolve the power exhaust issue in wireless sensor network. in the growing global requirements, the WSN has its own importance in all available fields in the physical world. Other then sensing the low power mode the sensors are being used many other applications for many purposes like temperature detection, pressure detection and also pollution detection. in order to save the energy of the nodes the constrained set them in sleep mode most of the time, which also increases the life spam of the nodes. the dos are the attacks which make the nodes to be in the state of wake up and effects the life span of the nodes. so, in this work we proposed a framework for the solution of such type of attacks through the detection of anti or malicious node.

7. Methodology to be Adopted

In our research we recommend a framework for power exhausting attacks in wireless sensor network. In the growing global requirements, the WSN has its own importance in all available fields in the physical world. Other then sensing the low power mode the sensors are being used many other applications for many purposes like temperature detection, pressure detection and also pollution detection. In order to save the energy of the nodes the constrained set them in sleep mode most of the time, which also increases the life spam of the nodes. The DoS are the attacks which make the nodes to be in the state of wake up and effects the life span of the nodes. So, in this work we proposed a framework for the solution of such type of attacks through the detection of anti or malicious node.

C. T. Hsueh et al. [13] proposed a framework; in this work author consider the power exhausting attacks in WSN to resolve the issue of lifetime of node(s) or complete network. For secure mechanism author consider SATCA to form hierarchical topology, it has four phases: -

1) Anti-Node detection
2) Cluster formation
3) Key distribution
4) Key renewal

In this work we extend the C. T. Hsueh work [13], to minimize the overhead and improve the security parameter for a same type of attacks in WSN. Key renewal phase create maximum overhead because key renewal means every time key is generated and distributed so to minimize the overhead we will not consider the key renewal phase and to maintain the security parameter we will consider RSSI (Receiving Signal Strength Indicator) value.

The RSSI (Received Signal Strength Indicator) value and the information about the routing is being combined together for the detection of the nodes which are malicious and also goes for checking the attackers identity. During the initial stage of the transmission there is a proper establishment of the path for routing and also for the computation of the RSSI values and recording the same. After that every node in the network confirms about the packet strength from the side of the source node. In the case when the RSSI value is not equal to the signal strength of the data packet that means the network has detected a malicious node.

And RSSI value of any node can be calculated as:

$$RSSI_i = E_t - 10\,\beta log_{10} l + \xi \quad (1)$$

Where Et is the transmit power of the node i (in dBm), β is the path loss exponent (a value between 2 and 4 chosen depending on the propagation environment), and ξ is a Gaussian distributed random variable with a mean of zero and a standard deviation σ up to 12 dB and l represents the distance from the node.

Phases of our proposed work:

1) Anti-node detection phase
2) Encrypted hello packet with RSSI value
3) Cluster formation
4) Key distribution

8. Expected Outcome of the Research

For finding security in WSN calculating security parameter of the proposed approach, existence of malicious node is estimated in certain circumstances and is used for the evaluation of results. We will estimate the security issue of node when malicious node may exist in network cause of denial of sleep attack. The RSSI (Received Signal Strength Indicator) value and the information about the routing is being combined together for the detection of the nodes which are malicious and also goes for checking the attackers identity. During the initial stage of the transmission there is a proper establishment of the path for routing and also for the computation of the RSSI values and recording the same. After that every node in the network confirms about the packet strength from the side of the source node. In the case when the RSSI value is not equal to the signal strength of the data packet that means the network has detected a malicious node. And for the security of data packet we encrypt it with a private key.

The Power of a sensor node(s) and security in WSN is essential as it helps in determining how probable a network is used for further transmission. And it helps in increasing the overall life and accuracy of the network.

For qualitative result, the proposed approach will be tested on few parameters: Security, utilization, time interval, traffic overhead. For performance comparison, the result of proposed work will be compared with existing work [13]. The results will explain that the proposed work helps in increasing the prevention of denial of sleep attack and security of the network. Therefore, the proposed work has higher security with low overhead.

9. Conclusion

Now, popularity of WSNs increases, and takes attention of many researchers. This paper treats security challenges in WSNs, which differ from the ad hoc networks with more severe restrictions in terms of energy, computation capabilities and communications. Consequently, the solutions of security must thus be adapted.

In this work, a study is being conducted for the security related issues for WSN, DoS attack is being considered for the research and the issues related to the power exhaust of the nodes in WSN is considered. The Power of a sensor node(s) and security in WSN is essential as it helps in determining how probable a network is used for further transmission. And it helps in increasing the overall life and accuracy of the network. RSSI (Receiving Signal Strength Indicator) value is being used in the proposal which detects the proper data about the nodes in the network, whether the node is malicious or not and also seeks to find the identity of the attacker node.

References

[1] I. F. Akyildiz, W. Su, Y. Sankara subramaniam, and E. Cayirci, "Wireless sensor networks: A survey", Computer Networks, 38(4), pp. 393–422, 2002.
[2] Sohraby, K., Minoli, D., Znati, "T. Wireless Sensor Networks: Technology, Protocols and Applications", John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2007.
[3] J A. Boukerche, "Algorithms and Protocols for Wireless, Mobile Ad Hoc Networks", John Wiley & Sons, Inc., 2009.
[4] Chiara, B., Andrea, C., Davide, D., Roberto, V, "An Overview on Wireless Sensor Networks Technology and Evolution", Sensors 2009, 9, pp. 6869-6896.
[5] *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.*
[6] Bharathidasan, A., Anand, V., Ponduru, S. (2001), "Sensor Networks: An Overview", Department of Computer Science, University of California, Davis 2001.
[7] *G. P. Halkes, T. V. Dam, and K. Langendoen,* "Comparing energy-saving MAC protocols for wireless sensor networks", *ACM Mobile Networks and Applications, 2005, Vol. 10, No. 5, pp. 783-791.*
[8] X. Chen and N. Rowe, "An Energy-Efficient Communication Scheme in Wireless Cable Sensor Networks", *Proc. of IEEE International Conference on Communications (IEEE ICC)*, June 2011.
[9] D.R. Raymond and S. F. Midkiff, "Clustered Adaptive Rate Limiting: Defeating Denial-Of-Sleep Attacks in Wireless Sensor Networks," *Military Communications Conference, 2007, MILCOM 2007, IEEE, pp. 1-7.*
[10] C. Chen, L.Hui, Q.Pei, L. Ning, P. Qingquan, "An Effective Scheme for Defending Denial-of-Sleep Attack in Wireless Sensor Networks," *Proceedings of the 2009 Fifth International Conference on Information Assurance and Security, Vol. 02, IEEE CS, 2009.*
[11] 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.*
[12] T. Bhattasali, R. Chaki, S. sanyal, "Sleep deprivation Attack Detection in Wireless Sensor network", *International Journal of Computer Applications, February 2012.*
[13] C.T. Hsueh, C. Wen, and Y. Ouyang, "A secure scheme against Power Exhausting Attacks in Hierarchal Wireless Sensor Network," *IEEE Sensor Journal, pp.1-13, 2015.*