INTERNATIONAL JOURNAL OF
RESEARCH IN COMPUTER
APPLICATIONS AND ROBOTICS
ISSN 2320-7345

A SURVEY ON DENIAL-OF-SLEEP-ATTACK IN WIRELESS SENSOR NETWORKS

Rojaramani M[1], Karpagam V[2], Keerthana K[3]

[1]PG Scholar, [2]Associate Professor, [3]PG Scholar
Sri Ramakrishna Engineering College, Coimbatore, Tamilnadu.

Abstract: - Security is an important issue nowadays in almost every network. Security and energy efficiency are critical concerns in wireless sensor network (WSN) design. Although various Media Access Control (MAC) protocols have been proposed to save the power and extend the lifetime of WSNs, the existing designs of MAC protocol are insufficient to protect the WSNs from Denial-of-Sleep attacks in MAC layer. Denial of sleep attacks are a great threat to lifetime of sensor networks as it prevents the nodes from going into sleep mode. In this paper we are describing prevention against Denials of sleep attack. We have analyzed each of proposed solutions, identify their strengths and limitations.

Index terms: Wireless Sensor Networks, Energy Efficiency, MAC Protocol, Denial-of-sleep attack

1. INTRODUCTION

Computer networks have grown in both size and importance in a very short time. If the security of the network is compromised, there could be serious consequences, such as loss of privacy, theft of information, and even legal liability. To make the situation even more challenging, the types of potential threats to network security are always evolving. It refers to any activities designed to protect your network. Specifically, these activities protect the usability, reliability, integrity, and safety of your network and data. Effective network security targets a variety of threats and stops them from entering or spreading on your network.

Wireless Sensor Networks are heterogeneous systems containing many small devices called sensor nodes and actuators with general-purpose computing elements. These networks will consist of hundreds or thousands of low cost, low power and self-organizing nodes which are highly distributed either inside the system or very close to it. These nodes consist of three main components-sensing, data processing and communication.

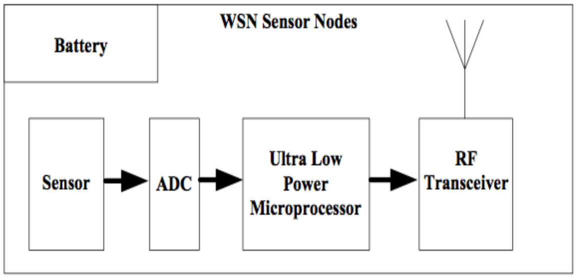

Fig.no.1 WSN Sensor Nodes

1.1 WIRELESS SENSOR NETWORKS

Wireless Sensor Networks (WSN) consists of several nodes where each node is connected to one or more sensor. Many people consider that wireless sensor network security is similar to WiFi applications. Compared to Wi-Fi, it needs real time deterministic performance. These are constrained in computational capabilities such as bandwidth and frequent powered battery changes. WSNs are easily accessible, have fixed field and are resistant to attacks. WSNs communication is very easy to attack. Some of the attacks on WSNs are eavesdropping, data injection and traffic analysis attacks. The combination of these factors demand security for sensor networks at design time to ensure security to operate, like secrecy of sensitive data and privacy to people in sensor nodes.

WSN Node
WSN Node
WSN Node
2.4 GHz, IEEE 802.15.4
WSN Gateway
Ethernet Cable

Fig.no.2 Communication between Wireless Sensor Nodes

1.2 ATTACKS IN WIRELESS SENSOR NETWORKS

There are many attacks which try to keep the sensor node awake so as to simply consume the energy of the nodes. Various attacks on sensor networks are:

- Denial-of-Sleep attack
- Hello attack
- Sybil attacks
- Selective Forwarding attacks
- Wormhole attacks

1.2.1 Denial-of-Sleep attack

It is a technique which prevents the radio from going into sleep mode. Many techniques introduced its impact on battery powered mobile devices. An attacker might use jamming attack to consume the energy and battery of the sensor but it would take about months to completely deplete the targeted devices whereas Denial-of-Sleep attack is a clever attack that keeps the sensor nodes radio ON that drain the battery in only few days. Several solutions have been proposed to solve these types of attack but each has limited features which are only concerned with the particular layer.

1.2.2 Hello attack

Numerous conventions oblige hubs to show Hello parcels to declare themselves to their neighbors, and a hub gaining such a bundle might accept, to the point that it is inside radio run of the sender. This supposition might be false: a portable computer class assaulter TV steering or other data with vast enough transmission power could persuade each hub in the system that the foe is its neighbor.

1.2.3 Sybil attack

It is one of the serious attacks on sensor network where sensor node illegitimately takes on multiple identities. This attack disturbs the aggression, fair resource allocation, and changes the routing. Some validation techniques may be undertaken to prevent this attack. Various prevention techniques are direct vs. indirect validation, identity vs. identity validation.

1.2.4 Selective forwarding attack

Multi-bounce systems are frequently dependent upon the presumption that taking part hubs will reliably forward gain messages. In a specific sending assault, noxious hubs might decline to send certain messages and basically drop them, guaranteeing that they are not engendered any further. A basic manifestation of this ambush is the point at which a malignant hub carries on as a dark opening and declines to advance each bundle.

1.2.5 Wormhole attack

In this assault, ambusher record parcel at one area of the system and tunnels them to an alternate area by retransmitting them. The least difficult occurrence of this assault is a solitary hub arranged between two different hubs sending messages between the two of them. Nonetheless, wormhole assaults more usually include two removed malevolent hubs plotting to understate their separation from one another by transferring parcels along an out-of-band channel accessible just to the aggressor. An ambusher arranged close to a base station may have the capacity to totally upset steering by making an overall put wormhole. An aggressor could persuade hubs who would regularly be numerous jumps from a base station that they are one and only or two jumps away by means of the wormhole. This can make a sinkhole: since the aggressor on the other side of the wormhole can falsely give a great track to the base station, conceivably all movement in the encompassing region will be drawn through if exchange tracks are fundamentally less engaging.

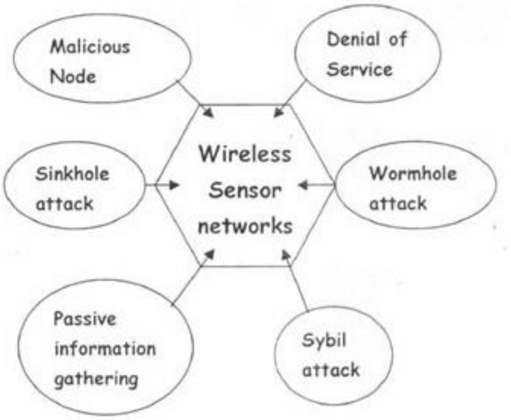

Fig.no.3 Security Attacks in Wireless Sensor Nodes

2. MAC PROTOCOL IN WSN

Communication in wireless sensor networks can, like most network communication, be divided into several layers. One of those is the Medium Access Control (MAC) layer. This layer is described by a MAC protocol, which tries to ensure that no two nodes are interfering with each other's transmissions, and deals with the situation when they do. Wireless sensor networks have an additional aspect: as sensor nodes are generally battery operated, energy consumption is very important. The radio on a sensor node is usually the component that uses most energy. Not only transmitting costs energy; receiving, or merely scanning the ether for communication, can use up to half as much, depending on the type of radio. While traditional MAC protocols are designed to maximize packet throughput, minimize latency and provide fairness, protocol design for Wireless Sensor Networks focus on minimizing energy consumption. The application determines the requirements for the (modest) minimum throughput and maximum latency.

2.1 Types of MAC Protocols

A. Sensor S-MAC

Sensor S-MAC,a contention based MAC protocol is modification of IEEE 802.11 protocol specially designed for the wireless sensor network in 2002. In this medium access control protocol sensor node periodically goes to the fixed listen/sleep cycle. A time frame in S-MAC is divided into to parts: one for a listening session and the other for a sleeping session. Only for a listen period, sensor nodes are able to communicate with other nodes and send some control packets such as SYNC, RTS (Request to Send), CTS (Clear to Send) and ACK (Acknowledgement). By a SYNC packet exchange all neighboring nodes can synchronize together and using RTS/CTS exchange the two nodes can communicate with each other.

B. Optimized MAC

In the Optimized MAC protocol, the sensors duty cycle is changed based on the network load. If the traffic is more than the duty cycle will be more and for low traffic the duty cycle will be less. The network load is identified based on the number of messages in the queue pending at a particular sensor. The control packet overhead is minimized by reducing the number and size of the control packets as compared to those used in the S-MAC protocol. This protocol may be suited for applications in which apart from energy efficiency there is need for low latency.

C. WiseMAC

The WiseMAC medium access control protocol was developed for the “WiseNET” wireless sensor network. This protocol is similar to Spatial TDMA and CSMA with Preamble Sampling protocol where all the sensor nodes have two communication channels. TDMA is used for accessing data channel and CSMA is used for accessing control channel. However, WiseMAC needs only one channel and uses non-persistent CSMA with preamble sampling technique to reduce power consumption during idle listening. This protocol uses the preamble of minimum size based on the information of the sampling schedule of its direct neighbors. The sleep schedules of the neighboring nodes are updated by the acknowledgement message (ACK) during every data transfer. WiseMAC is adaptive to the traffic loads and provides low power consumption during low traffic and high energy efficiency during high traffic.

D. Berkeley a Access Control (B-MAC)

The Berkeley Media Access Control (B-MAC) is a contention based MAC protocol for WSNs. B-MAC is similar to Aloha with Preamble Sampling, which duty cycles the radio transceiver i.e. the sensor node turns ON/OFF repeatedly without missing the data packets. However in B-MAC, the preamble length is provided as parameter to the upper layer. This provides optimal trade-off between energy savings and latency or throughput. The paper also presents an analytical model for monitoring application to calculate and set B-MAC parameters in order to optimize the power consumption.

E. Self Organizing Medium Access Control for Sensor Networks (SMACS)

SMACS is a schedule based medium access control protocol for the wireless sensor network. This MAC protocol uses a combination of TDMA and FDMA or CDMA for accessing the channel. In this protocol the time slots are wasted if the sensor node does not have data to be sent to the intended receivers.

3. RELATED WORKS

In this section, a general survey is conducted of the recent works related to energy consumption in wireless sensor networks.

In [2],It classifies Denial-of-Sleep attacks on WSN MAC protocols based on an attacker's knowledge of the MAC protocol and ability to penetrate the network. The impacts on sensor networks running four leading WSN MAC protocols (S-MAC,T-MAC,B-MAC,G-MAC) is analyzed for the efficiency of implementations of attack. It proposes a Defensive framework for defending against Denial-of-Sleep attack. It incorporates four key components strong link-layer authentication, anti-replay protection, jamming identification and mitigation and broadcast attack defense. The Advantage is Explores physical layer jamming, intelligent replay and a full domination attack for each of the S-MAC,T-MAC,B-MAC,G-MAC protocols considered. But Disadvantages is Defensive framework provided for only four of the MAC Protocols are S-MAC,T-MAC,B-MAC, and G-MAC.

In [11],Defense algorithm is proposed to detect and mitigate Denial- of –Sleep attack. This algorithm uses a detection mechanism with a simple defense technique and merges them with MAC's procedures. It forces nodes to enter into deep sleep cycle when abnormal activities are detected. However, due to their simplicity structured (CPU & memory) they need special procedures to deal with those attacks. This research focuses on the attacks that are aimed at power resources which are referred as Denial of Sleep attacks. The Advantages is it saves node's power and makes the attacker to drain its power. It Does not require complex processing. And so Disadvantages are attacked nodes which enter deep sleep mode will be excluded from the network temporarily and may affect data flow in the network.

In [7],A cross-layer design considers the joint optimization of MAC and routing layers has been proposed. At the routing layer, a life-optimal routing algorithm takes advantage of the total available energy resources in the network before its death. At the MAC layer, is controlled the retry limit of retransmissions over each wireless link. The Advantages is Energy Conservation can be achieved. Load balancing traffic through the WSN.To improve network lifetime. But Disadvantage are at the network layer proposing new routing solutions that take into account the sleep state of some nodes.

In [5], A Systematic and comprehensive taxonomy of the energy conservation schemes is used. Duty cycle is defined as the fraction of time nodes which are active during their lifetime. Data driven approaches can be used to improve the energy efficiency even more. Data-driven approaches

Can be divided to data reduction schemes to address the case of unneeded samples, while energy-efficient data acquisition schemes are mainly aimed at reducing the energy spent by the sensing subsystem. The Advantages is Reduces the time where the sensor is being idle. And Disadvantages is Additional delay because of waiting for the next-hop node to wake up.

In [9],Secure decentralized clustering algorithm for wireless ad-hoc sensor networks. Based on the cluster-based topology, secure hierarchical communication protocols and dynamic quarantine strategies are introduced to defend against spam attacks. This type of attacks can exhaust the energy of sensor nodes and will shorten the lifetime of a sensor network drastically. By adjusting the threshold of infected percentage of the cluster coverage, the scheme can dynamically coordinate the proportion of the quarantine region and adaptively achieve the cluster control and the neighborhood control of attacks. The Advantages is to protect the network from energy-exhaustion attacks. And Disadvantages is does not identify anti-network sensors and No efficient security mechanisms to make protocol suitable for adaptive topology management.

4. CONCLUSIONS

Wireless sensor network is used in different types of applications due to tremendous growth. Hence security and reliability becomes the main concern in every wireless sensor network applications. This paper described WSN, several possible Denials of sleep attacks, some of the types of denial of sleep attack and MAC protocols in WSN. We analyzed several currently available solutions; identify their strengths and limitations and provide comparison among them.

REFERENCES

[1] C.-T. Hsueh, Y.-W. Li, C.-Y. Wen and Y.-C. Ouyang, "Secure adaptive topology control for wireless ad-hoc sensor networks," *Sensors*, vol. 10,no. 2, pp. 1251–1278, 2010.

[2] 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.

[3] Fatma Bouabdallah, Nizar Bouabdallah and Raouf Boutabaz," Cross-Layer Design for Energy Conservation in Wireless Sensor Networks," in Proc INRIA, Campus universitaire de Beaulieu ; 35042 Rennes Cedex, France. (z)School of Computer Science, University of Waterloo; 200 University Ave. W., Waterloo, ON, Canada.

[4] 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.

[5] Giuseppe Anastasi, Marco Conti, Mario Di Francesco, Andrea Passarella," Energy conservation in wireless sensor networks: A survey," in Proc. Ad Hoc Networks 7 (2009), pp. 537–568.

[6] J. Polastre, J. Hill, and D. Culler, "Versatile low power media access for wireless sensor networks," in Proc. 2ndInt. Conf. Embedded Netw. Sensor Syst. (SenSys), Baltimore, MD, USA, 2004, pp. 95–107.

[7] K.-T. Chu, C.-Y. Wen, Y.-C. Ouyang, and W. A. Sethares, "Adaptive distributed topology control for wireless ad-hoc sensor networks," in Proc. Int. Conf. Sensor Technol. Appl. (Sensor Comm), Valencia, Spain,2007, pp. 378–386.

[8] 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.

[9] 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.

[10] M. Li, Z. Li, and A. V. Vasilakos, "A survey on topology control in wireless sensor networks: Taxonomy, comparative study, and open issues," Proc. IEEE, vol. 101, no. 12, pp. 2538–2557, Dec. 2013.

[11] M. Wainis, K. Kabalan, and R. Dandeh," Denial of Sleep Detection and Mitigation," in proc. Latest Trends on Communications. ISBN: 978-1-61804-235-4.

[12] R. C. Carrano, D. Passos, L. C. S. Magalhaes, and C. V. N. Albuquerque, "Survey and taxonomy of duty cycling mechanisms in wireless sensor networks," IEEE Commun. Surv. Tuts., vol. 16, no. 1, pp. 181–194, First Quarter 2014.

[13] T. van Dam and K. Langendoen, "An adaptive energy-efficient MAC protocol for wireless sensor networks, "in Proc. 1st Int. Conf. Embedded Network Sensor Syst. (SenSys), Los Angeles, CA, USA, 2003, pp. 171–180.

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

[15] 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 Network .Sensor Syst. (SenSys), Raleigh, NC, USA, 2008, pp. 1–14