International Journal of Advance Research in Science and Engineering
Vol. No.5, Issue No. 02, February 2016
www.ijarse.com
IJARSE
ISSN 2319 - 8354

METHOD TO IMPROVE ENERGY IN DENIAL OF SLEEP ATTACK

Kalyani Vaidya[1], Kailash Jadhao[2]

[1]Student, [2]Guide, EXTC, Mumbai University, (India)

ABSTRACT

Attackers use their knowledge of their underlying MAC protocol, to reduce the sleep time of the node, so that life time of the node reduces. As constant traffic is not necessary ,the attack is sometimes hard to detect.Various Denial of sleep attacks can target MAC protocols,because they control the transceiver .MAC protocols dictate the transceiver when to transmit packets,when to listen to the channel and when to sleep.Most protocols were designed in order to conserve energy by putting the transceiver to sleep for long periods of time. Various protocols are designed to reduce the energy consumption of sensor nodes by keeping the antenna in sleep mode 90% of time, so that power is saved MAC protocols are designed to vary the sleep time based on the communication need. However this problem we refer it as Denial of sleep attack and in this paper we propose effective solution to defend against this attack on a sensor network. The existing system is based on Packet threshold analysis mechanism used for detection of attack here.The proposed system is based on Challenge response security activated to ensure the validity of the sender here and prevent unwanted communication between the nodes.

Keywords: *Security; Sensor networks; Denial of sleep attack; MAC protocols.*

I. INTRODUCTION

Wireless sensor network (WSN) consist of several nodes where each node is connected to one or more sensor. WSN have applications in many important areas, such as the military, homeland security, health care, the environment, agriculture, and manufacturing. Providing security in Sensor networks are not an easy task. Compared to conventional desktop computers, severe constraints exist since sensor nodes have limited processing capability, storage, and energy, and wireless links have limited bandwidth.

The most energy consumption attack in WSN is denial of sleep attack in which attacker consumes the sensor nodes energy by making it nodes wake even when there is no traffic to hold. In this way sensor nodes energy is consumed totally and sensor nodes die. Due to which the lifetime of the wireless sensor network decreases by causing the radio of the receiver ON draining the battery in only few days. Energy is wasted due to Collision, Overhearing, and Control packet overhead and Over-emitting. When the receiver node receives more than one packet at a time collision occurs and has to be discarded and retransmitted which increases the energy consumptions. Overhearing occurs when the node receive a packet destined for other node which causes the receiving node energy consumption by keeping its radio on. The third energy consumption problem is control packet overhead where the minimum number of control packets are send for the data transmission as the staying the node wake for control packets consume the battery life

1.1 Various Types of Attack

Most of the research in WSN security has concentrated on the confidentiality and integrity of the data in the network. Due to the limited energy of a WSN, it remains extremely vulnerable to security attacks draining the most critical resource. Different security attacks, which amplify the energy drains and delays, can majorly affect the performance of the MAC layer. The effect of these attacks on the MAC layer performance can be minimized or removed, if the behavior of the

attacks is analyzed and modeled. It enlightens the sequence of activities perform by attacker or malicious node. The following subsections explain the main MAC security attacks in detail.

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 uses 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 [10]. Several solutions have been proposed to solve these types of attack but each has limited feature which are only concern to the particular layer

2) Collision Attack

The malicious collision attack can be easily launched by a compromised sensor node. In a collision attack, a malicious node does not follow the MAC protocol rules and causes collisions with neighboring nodes' transmissions by sending a short noise packet. This attack does not consume much energy of the attacker but can cause a lot of disruptions to the network operation. It is difficult to detect this attack because of the broadcast nature of the wireless environment.

3) Unintelligent Attack

In case of the unintelligent replay attack, the attacker does not have MAC protocol knowledge and no ability to penetrate the network. Here, recorded events are replayed into the network which prevent nodes from entering sleep mode and lead to waste in energy in receiving and processing the extra packets. If nodes are not equipped with an anti-replay mechanism attack causes the replayed traffic to be forwarded through the network, consuming power at each node on the path to

the destination. The replaying of events has adverse effect on the network lifetime and overall performance of WSN.

4) Unauthenticated Broadcast attack

In an unauthenticated broadcast attack, the attacker has full knowledge of the MAC protocol but does not have the capability to penetrate the network. Here, the attacker broadcasts the unauthenticated traffic into the network by following all MAC rules. These unauthenticated and unnecessary broadcasts messages are disturbing the normal sleep and listen cycle of the node and place most of the nodes in listen mode for an extended amount of time; it leads to increase in

energy consumption and reduction in network lifetime. These attacks cause server harm to MAC protocols that are having short messages and short adaptive timeout period.

5) Full Domination attack

Here, the attacker has full knowledge of the MAC layer protocol and ability to penetrate the network. This type of attack is one of the most destructive to a WSN as the attacker has the ability to produce trusted traffic to gain the maximum possible impact from denial of sleep. The attacks are mounted using one or more compromised nodes in the network. All kinds of MAC layer protocols are vulnerable to this kind of attack.

6) Exhaustion attack

The attacker who commences an exhaustion attack has knowledge about the MAC protocol and the ability to penetrate the network. These attacks are possible only in case of request to send (RTS)/clear to send (CTS) based MAC protocols. In this attack, the malicious node sends RTS to a node and if the node replies with CTS, the malicious node will repeatedly transmit the RTS to the node, which will prevent the node from going into sleep mode and instead drain the total energy of the node. These attacks are affecting the node lifetime and can partition the network.

7) Intelligent Jamming attack

The intelligent jamming attack is one of the most disastrous attacks where attacker has full protocol knowledge but does not have the ability to penetrate the network. The attacker injects unauthenticated unicast and broadcast packets into the network. These attacks can differentiate between control traffic and data traffic and unlike the unauthenticated replay attack it replays the selective events (control or data)

1.2 WSN Operation

Wireless sensor network (WSN) is the collection of homogenous, self-organized nodes called sensor nodes. These nodes have the capabilities of sensing, processing and communication of data with each other wirelessly using radio frequency channel. The basic task of sensor networks is to sense the events, collect data and send it to their requested destination. Many of the features of these networks make them different from the traditional wired and wireless distributed systems. Traditional wired or wireless networks have enough resources like unlimited power, memory, fixed network topologies, enough communication range and computational capabilities. These features make the traditional networks able to meet the communication demands [10]. On the other hand, WSNs are resource constrained distributed systems with low energy, low bandwidth and short communication range. The basic features which make WSNs different from the traditional networks are; self-organizing capabilities, short range communication, multi-hop routing, dense deployment, limitation in energy and memory, and also frequently changing topology due to fading and failures. The constrained resource nature and unpredictable network structure (sensor nodes are scattered densely in an environment) poses numerous design and communication challenges for WSNs. According to [10] “The challenges in the hierarchy of: detecting the relevant quantities, monitoring and collecting the data, assessing and evaluating the information, formulating meaningful user displays, and performing decision-making and alarm functions are enormous.” Generally, the wireless sensor network operation involve data acquisition and data reporting therefore it has a data acquisition network and data distribution network and a management center responsible for its monitoring and control as shown in Figure 1 below.

II. BLOCK DIAGRAM OF SYSTEM

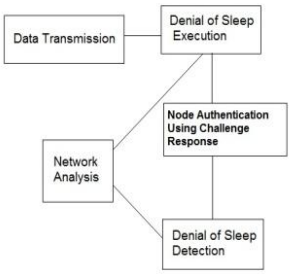

Fig 1. Block Diagram of Denial of Sleep Attack

In denial of sleep attack, goal of the intruder is to maximize the power consumption of the sensor node, thereby decreasing its battery life. The attack achieves this by keeping the sensor node busy and preventing it from going into low power sleep mode. An attacker can exhaust a node's resources by repeatedly sending RTS messages triggering CTS responses from a targeted node. In this case, all the nodes within the radio range of the sender will be receiving those (RTS) control packets, thus draining their power supplies. The attacker may also send a constant stream of unauthenticated or replayed broadcast packets causing the nodes to remain awake.

III. CHALLENGES OF SECURITY IN WSNS IN DENIAL OF SLEEP ATTACK

Resource constraints

- limited computational, networking, and storage capabilities of sensors
- energy constraints of sensors
- Lack of central control
- large WSNs often don't have centralized control
- requires distributed/decentralized security solutions
- Remote location
- Sensors often left unattended
- difficult to prevent unauthorized physical access and tampering
- Error-prone communication
- difficult to distinguish wireless communication errors from attacks
- A sensor network should not leak sensor readings to its neighbors..
- In many applications nodes communicate highly sensitive data, e.g. key distribution, therefore high security
- Public sensor information, such as sensor identities and public keys, should also be encrypted protect against traffic analysis attacks.
- Sensitive data secret is encrypted with a secret key that only intended receivers possess, for confidentiality.

IV. LITERATURE SURVEY

In these previous papers, these various methods were used for authentication:

1) Gateway node was used to carry out Registration, Login, and Authentication.

2) Public key cryptography was used but the disadvantage is that it is power consuming

3) Sensor communicates among each other with the help of symmetric cryptography.

4) Sensors in the communication range serve as promoters between public key cryptography of the user and symmetric crypto world of WSN

V. PROBLEM DEFINITION

Wireless sensor network Wireless sensor network (WSN) is vulnerable to attacks due its energy constraints. Wireless sensor network consists of several nodes where each node is connected to one or more sensor. Due to limited range, power, and processing constraints and its cost sensors are out of reach of real world. Other than this, there are large number of nodes in a network which lacks their global id and are prone to failure. For conserving the energy of sensor network, there is a modes of wsn nodes. Various modes are active mode and sleep mode. Active mode of wsn node is to show that wsn node is ready to receive and send data. Whereas, sleep mode show that wsn node is not ready to receive or send the data. There are diferent levels of energy consumption in each of modes.

VI. PROPOSED SYSTEM

To identify denial of sleep attack for preventing continuous depletion of energy of the proposed destination in a particular network structure. The detection process will include generation of public key at authority node and utilization of hash signature for detection of the same at the destination node using secret key at destination node. Thereby, preventing depletion of energy during transmission.

VII. DESIGN STEPS

The following modules will be implemented:

1. Network Configuration and Creation: This module will involve designing the network structure to be used for transmission.
2. Denial of Sleep attack: This module will demonstrate execution of denial of sleep attack wherein the node energy will be depleted due to existence of an attack node. Due to this depletion of energy, the overall performance of the network will be affected and therefore, degraded transmission executes. It will involve transmission of data from source to destination node and its analysis to track the details of nodes.
3. Denial of Sleep Detection using challenge and response concept: This module will facilitate the execution of denial of sleep and its detection using authentication mechanism. This mechanism will involve attachment of a hashed signature with the data transmitted will be distributed using an Authentication Node.
4. Analysis Module: This module will facilitate the generation of analysis of transmission time of the above executions and get an overall view of the performance of the network on the basis of transmission time (i.e avg. residual energy in terms of time)

VIII. SIMULATION

Software Environments

Simulation Tool

The software used in the project for investigating the performance of MANET routing protocols is NS-2.34.NS-2.34 is a discrete event network simulator that has begun in 1989 as a variant of the REAL network simulator. Initially intended for wired networks, the Monarch Group at CMU have extended NS-2.34 to support wireless networking such as MANET and wireless LANs as well. Most MANET routing protocols are available for NS-2, as well as an 802.11 MAC layer implementation. NS-2's code source is split between C++ for its core engine and OTcl, an object oriented version of TCL for configuration and simulation scripts. The combination of the two languages offers an interesting compromise between performance and ease of use.

Implementation and simulation under NS-2.34 consists of 4 steps:

Implementing the protocol by adding a combination of C++ and OTcl code to NS-2's source base;

Describing the simulation in an OTcl script;

Running the simulation and Analyzing the generated trace files

Network Simulator (Version 2.34), widely known as NS2.34, is simply an event driven simulation tool that has proved useful in studying the dynamic nature of communication networks. NS2 consists of two key languages: C++ and Object-oriented Tool Command Language (OTcl). While the C++ defines the internal mechanism (i.e., a backend) of the simulation objects, the OTcl sets up simulation by assembling and configuring the objects as well as scheduling discrete events (i.e., a frontend) [12].

Implementing a new protocol in NS-2 typically requires adding C++ code for the protocol's functionality, as well as updating key NS-2 OTcl configuration files in order for NS -2 to recognize the new protocol and its default parameters. The C++ code also describes which parameters and methods are to be made available for OTcl scripting. The NS-2 architecture follows closely the OSI model. We have adapted the implementation of flooding provided in NS-2 in the context of diffusion in sensor networks .An agent in NS-2 terminology represents an endpoint where network packets are constructed, processed or consumed. Such an Agent was implemented at the Application layer for the broadcast source, and the simulation trace was collected at the MAC layer. Some disadvantages of NS-2 stem from its open source nature. First, documentation is often limited and out of date with the current release of the simulator. Fortunately, most problems may be solved by consulting the highly dynamic newsgroups and browsing the source code. Then code consistency is lacking at times in the code base and across releases. Finally, there is a lack of tools to describe simulation scenarios and analyze or visualize simulation trace files. These tools are often written with scripting languages. The lack of generalized analysis tools may lead to different people measuring different values for the same metric names. The learning curve for NS-2 is steep and debugging is difficult due to the dual C++/OTcl nature of the simulator. A more troublesome limitation of NS-2 is its large memory footprint and its lack of scalability as soon as simulations of a few hundred to a few thousand of nodes are undertaken.

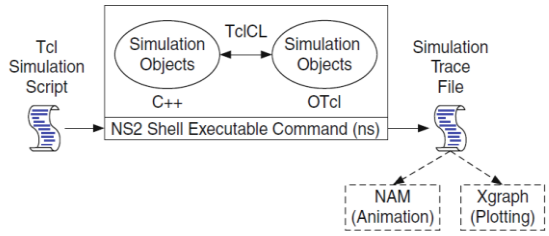

Figure 2.NS-2 Architecture

TCL Script. (path.tcl)

TCL Script **(path.tcl)** which we are using defines all nodes and all required parameters.

```
set val(chan)   Channel/WirelessChannel    ;# channel type
set val(prop)   Propagation/TwoRayGround   ;# radio-propagation model
set val(netif)  Phy/WirelessPhy            ;# network interface type
set val(mac)    Mac/802_11                 ;# MAC type
set val(ifq)    Queue/DropTail/PriQueue    ;# interface queue type
set val(ll)     LL                         ;# link layer type
set val(ant)    Antenna/OmniAntenna        ;# antenna model
set val(ifqlen) 512                        ;# max packet in ifq
set val(nn)     67                         ;# number of mobile  nodes
set val(rp)     AODV                       ;# routing protocol
set val(x)      4300                       ;# X dimension of topography
set val(y)      2500                       ;# Y dimension of topography
set val(stop)   20.0                       ;# time of simulation end
set ns [new Simulator]
set topo [new Topography]
$topo load_flatgrid $val(x) $val(y)
create-god $val(nn)
#Open the NS trace file
set tracefile [open path.tr w]
$ns trace-all $tracefile
$ns use-newtrace
set namfile [open path.nam w]
$ns namtrace-all $namfile
$ns namtrace-all-wireless $namfile $val(x) $val(y)
set chan [new $val(chan)];#Create wireless channel
```

NAM file i.e Network Animator File (path.nam)

When a simulation is finished, NS produces one or more text-based output files that contain detailed simulation data, i.e **path.nam** if specified to do so in the input Tcl (or more specifically, OTcl) script. The data can be used for simulation analysis (two simulation result analysis examples are presented in later sections) or as an input to a graphical simulation display tool called Network Animator (NAM). NAM has a nice graphical user interface

similar to that of a CD player (play, fast forward, rewind, pause and so on), and also has a display speed controller. Furthermore, it can graphically present information such as throughput and number of packet drops at each link, although the graphical information cannot be used for accurate simulation analysis.

Location Details (location-anchor1)

Another text based file is generated after end of simulation which gives the desired location of all nodes. Like Source, Neighbor, SX-Pos, SY-Pos, Distance(d)

IX. FUTURE SCOPE

Most current research in WSN security focuses on data confidentiality and integrity, largely ignoring availability. Without the ability to secure the physical medium over which communication takes place, sensor networks are susceptible to an array of potential attacks focused on rapidly draining sensor node batteries, thereby rendering the network unusable.

The three contributions to the area of sensor network security are first, 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. Second, it explores potential attacks from each attack classification, both modeling their impacts on sensor networks running four leading WSN MAC protocols and analyzing the efficiency of implementations of these attacks on three of the protocols. Finally, it proposes a framework for defending against denialof- sleep attacks and provides specific techniques that can be used against each denial-of-sleep vulnerability. Future work and finding ways to apply it to currently available sensor devices to further develop specific mechanisms to protect them against these attacks.

As wireless sensor networks continue to grow and become more common, we expect that further expectations of security will be required of these wireless sensor network applications. In particular, the addition of public key cryptography and the addition of public-key based key management will likely make strong security a more realistic expectation in the future. We also expect that the current and future work in privacy and trust will make wireless sensor networks a more attractive option in a variety of new arenas**.**

X. CONCLUSION

10.1 Performance Evaluation

We will simulate the energy efficient localization technique on Network Simulator (version 2.3.4) widely known as NS2 [12], a scalable discrete-event driven simulation tool.

Building high performance WSN network systems requires an understanding of the behavior of sensor network and what makes them fast or slow. In addition to the performance analysis, we have also evaluate the proposed technique in which denial of sleep attack between nodes will be detected and prevented with the help of new technique ,challenge response method. The final but most important step in our experiment is to analyze the output from the simulation. After the simulation we obtain the trace file from the simulation.

REFERENCES

[1] Manju.V.C Senthil Lekha.S. L. Dr.Sasi Kumar M." Mechanisms for Detecting and Preventing Denial of Sleep Attacks on Wireless Sensor Networks.

[2] Zhang Shaoping, Li Guohui, Wei Wei and Yang Bing, "A Novel Iterative Multilateral Localization Algorithm for Wireless Sensor Networks", Journal of Networks,Vol.5,No.1,pp.112-119,Jan2010.

[3] Yuan Zhu, Baoli Zhang and Shufeng Ning, "A RSSI based localization algorithm using a mobile anchor node for wireless sensor networks", International Joint Conference on Computational Sciences and Optimization, 2009.

[4] Wojciech Zajdel, Ben J.A. Krose, Nikos Vlassis, "Bayesian y of Amsterdam, 2005.

[5] Anouar.A.Boudhir and Ben Ahmed Mohamed, "New technique of Wireless Sensor Networks Localization based on energy consumption", IJCA Vol.9- 12, Nov 2010.

[6] W.H.Liao, Y.C.Lee and S.P.Kedia, " Mobile anchor positioning for Wireless Sensor Networks", IET Communications, Aug 2010.

[7] Jasper Gnana Chandran.J and S.P.Victor," An energy efficient localization technique using particle swarm optimization in mobile wireless sensor networks. American Journal of Scientific Research ISSN 1450-223X Issue 8, pp. 33-48, 2010.

[8] Frankie K.W.Chan, H.C.So and W.K.Ma, "A novel subspace approach for Co-operative Localization in Wireless Sensor Networks using Range measurements", IEEE Transactions on Signal Processing, IEEE Computer society, Vol.57, No.1, pp. 260-269, Jan 2009.

[9] Z. Zhong and T. He, "Achieving range-free localization beyond connectivity," in SenSys, 2009.

[10] Teerawat Issariyakul and EkramHossain, "Introduction to Network Simulator NS2", ISBN: 978-0 - 387-71759-3, Springer Science + Business Media, LLC, 2009.