RESEARCH ARTICLE OPEN ACCESS

Cryptosystem to Overcome Misdirection Attack in Wireless Sensor Network

Chythra M[1], B R Prasad Babu[2], Ashok K Patil[3]
M-tech Student[1] , Professor & Head[2]. , Associate Professor[3]
Dept of CSE, R&D Center,EPCET, Bangalore

Abstract:

Now a day's wireless sensor network are the preferred filed to use, but it often prone to different security threats. This paper takes a look on different types of attack and the RSA encryption, decryption method to overcome the misdirection attack with DSDV protocol. Simulation helps to identify the packet delivery ratio, throughput and also Bit error rate.

Keywords — **Wireless sensor network, Denial of service, Destination-Sequenced Distance vector,Tool command language**

I. Introduction

A wireless sensor network is a remote system comprising of spatially conveyed self-sufficient gadgets utilizing sensors to screen physical or ecological conditions. WSN is heterogynous framework; its imperative components resemble restricted battery, constrained power and restricted stockpiling. A WSN framework consolidates an entryway that gives remote network back to the wired world and circulated nodes. The benefits of WSN are versatility, adaptability and robustness. This present reality utilizations of WSN are natural checking, military applications, medicinal observing and activity observing.

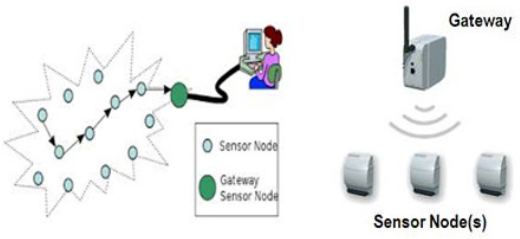

Fig1: Architecture of WSN

The various security requirements for WSN are…Data confidentiality, data integrity, data availability, data authentication and data freshness. The most significant issue in network security is data confidentiality.

II. Clustering method

The objective of clustering is to decrease the measure of information by sorting or gathering comparative information things together. There are two basic types of clustering method…Hierarchical and Partitional clustering.

A. Hierarchical clustering: Hierarchical grouping (likewise called various leveled cluster examination or HCA) is a strategy for cluster investigation which looks to fabricate a hierarchy of cluster.

B. Partitional clustering endeavors to straightforwardly break down the information set into an arrangement of disjoint clusters. The basis work that the clustering calculation tries to minimize may underline the neighborhood structure of the information, as by allotting clusters to crests in the likelihood thickness capacity, or the worldwide structure.

II. Types of Attack

Denial of Service attack: Denial of service (DoS) attack is an endeavor to make a machine or system asset occupied to its expected clients, for example, to incidentally or inconclusively hinder or suspend administrations of a host associated with the Internet.

Sinkhole attack: In a sinkhole attack an interloper bargains a node or presents a node inside the system and uses it to dispatch an attack. The traded off node tries to attack all the activity from neighbor nodes taking into account the directing metric utilized as a part of the steering convention. Sinkhole attack are a sort of network layer attack where the traded off node sends fake steering data to its neighbor's to attack network activity to itself. WSNs are especially Vulnerable to sinkhole attack.

Worm hole attack: Worm hole attack is one of the denial of administration attack that can influence the network even without the Knowledge of cryptographic procedures executed. This is the motivation behind why it is exceptionally hard to detect. it might be dispatched by one, two or more number of nodes. In two ended worm hole packets are burrowed through worm hole link from source to destination.

Misdirection attack: Misdirection a sort of Denial of Service (DoS) attack is extremely hard to distinguish and guard. In misdirection attack, the interloper misleads the approaching parcels to a node other than the expected node. Because of this attack, top of the line to-end delay (at times boundless) is presented in the network and execution of the network (i.e. throughput) is debased.

III. RSA(Cryptosystem):

Misdirection assault is one of the refusals of administration assault where the malignant nodes mislead the packet transmission to various nodes which is not a correct destination. Due to malignant node between the intermediate nodes the packet will not reach the correct destination which leads to a huge packet loss. This also reduces the packet delivery ratio, throughput and also increases bit error rate.

Encryption and Decryption

The nodes are grouped in the cluster based on the energy. The node having highest energy will be selected as cluster head. Cluster head is formed based on the cluster head selection algorithm. The data transmission takes place in an optimum path i.e. the shortest path will be selected to transfer data based on the database.

Due to unavoidable conditions the data before transmission is hidden from the unauthorized user by the technique of encryption. There will not be any data loss during transmission due to encryption methodology. The destination node will receive the data within the stipulated time with no packet loss. The hidden information will be revealed at the destination by the method of decryption.

The process of encryption and decryption is known as cryptosystem. RSA algorithm is used in this system to avoid the packet loss during transmission. The DSDV algorithm is used in this process in order to increase the throughput and packet delivery ratio.

DSDV protocol

The Destination-Sequenced Distance Vector (DSDV) protocol is the usually utilized proactive steering protocol in mobile ad hoc network (MANET). In DSDV, every node keeps up a steering table with one course section for every destination in which the most limited way is recorded. It utilizes a destination arrangement number to abstain from directing loops.

The sample code of encryption and decryption with DSDV protocol

```
proc RSA {} {
#!/usr/bin/tclsh

# Tcl program to encrpyt and decrypt a file using RSA

# initialize the parameters for RSA algorithm
set e 3
set d 11787
set n 17947
# accept the user's choice
puts "Enter 'E' to encrpyt or 'D' to decrypt"
set choice [gets stdin]
set choice [string toupper $choice]
if {$choice eq "E"} {

# accept the name of the file to encrypt from the user
puts "Enter the absolute path of the file to be encrypted :\t"
set fname [gets stdin]
puts "ENCRYPTION IN PROGRESS ....."
set new [split $fname {.}]
set newfile [lindex $new 0]

# open the file in read mode
set fileid1 [open $fname r]

# open another file in write mode
append newfile "_crypt.txt"
set fileid2 [open $newfile w]

# read the input file
set cont [read $fileid1]
close $fileid1

#split the file contents into constituent characters
set mylist [split $cont {}]

# process character-wise and encrypt
foreach {char} $mylist {
        set asc [scan $char %c] ; # scan command here is used to convert char to ascii
        set res 1
        for {set i 1} {$i <= $e} {incr i} {
                set res [expr "($res * $asc) % $n"]
        }
        set newchar [format "%c" $res]
        puts -nonewline $fileid2 $newchar
}
close $fileid2
puts "ENCRYPTION COMPLETE, It is using the RSA fuction,encrypted part is avaliable in _crypt.txt....."
}


if {$choice eq "D"} {
# Tcl program to decrpyt a file using RSA

# initialize the parameters for RSA algorithm

set e 3
set d 11787
set n 17947

# accept file name to decrypt
```

```
puts "Enter the absolute path of the file to be decrypted :\t"
set fname [gets stdin]
puts "DECRYPTION IN PROGRESS sucessfully decrypted,and saved in _decrypt.txt....."
set new [split $fname {.}]
set newfile [lindex $new 0]

# open the file in read mode
set fileid1 [open $fname r]

# open another file in write mode
append newfile "_decrypt.txt"
set fileid2 [open $newfile w]
# read the input file
set cont [read $fileid1]
close $fileid1

#split the file contents into constituent characters
set mylist [split $cont {}]

# process character-wise
foreach {char} $mylist {
        if {$char eq ""} {break}
        set asc [scan $char %c]
        set res 1
        for {set i 1} {$i <= $d} {incr i} {
                set res [expr "($res * $asc) % $n"]
        }
        set newchar [format "%c" $res]
        puts -nonewline $fileid2 $newchar
}
close $fileid2
puts "DECRYPTION COMPLETE ....."
}
```

Simulation process

NS-2 is a network simulator version 2.It is a discrete event simulator for networking research work at packet level. It is a discrete event simulator for networking research work at packet level.

It also provides substantial support to simulate bunch of protocols like TCP, UDP, FTP, HTTP and DSR.NS2 is primarily Unix based. It uses TCL(Tool command language) as its Scripting language.

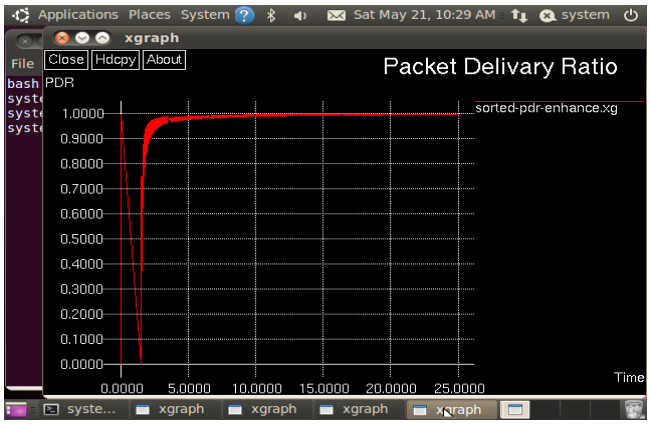

Fig 2: Packet Delivery Ratio

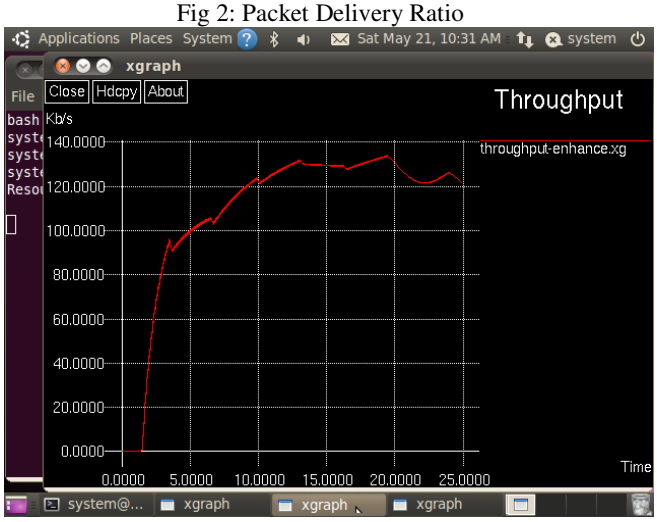

Fig 3: Throughput

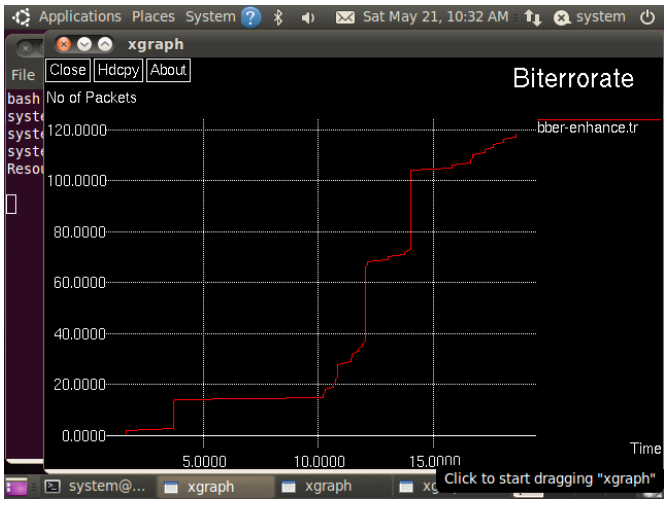

Fig 4: Bit Error Rate

IV. References

[1] IJCA special Issue on “mobile Ad-hoc Networks” MANETs,2010

[2] International Journal on Adhoc networking systems vol.2,no.4,october 2012.

[3] Roshan singh sachan;Department of CSE,graphic Era University Dehradun,India.

[4] “Survey on clustering technique in wireless sensornetwork” by RudranathMitra,DiyaNandy.

[5] “Intoduction to clustering tehniques” by leo wanner.

[6] RSA(cryptosystem) from Wikipedia, the free encyclopedia.