International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 24 Issue 9 – JUNE 2017.

Mitigating Denial of Service attacks in Dynamic Source Routing protocol

Krishnamurthi[#1] H Srinivas Murthy and Bharathi M [*2]

[#] *Department of CSE,SJCIT, Chickballapur, Karnataka, India.*

***Abstract*— A Wireless Sensor Networks consists of sensor nodes that capture information from an environment, processing data and transmitting them via radio signals, for this communication among node is an important aspect ,Hence the primary requirement for the establishment of communication among nodes is that each node should cooperate with each other, but in the presence of malevolent nodes, this requirement may lead to serious security concerns; for instance such node may disrupt the routing process. In this context preventing or detecting malicious nodes launching denial of service attack or collaborative black hole attack is a challenge. This paper attempts to resolve this issue by using various algorithms in order to provide security in terms of confidentiality, integrity and reliability in terms of transmission of data.**

The final output shows simulating results of various network parameters like Throughput, Average delay, Probability of bandwidth utilization, Network failure rate in NS2 simulator.

***Index Terms*— WSN, DOS attack, Black hole attack, throughput,Average delay, Bandwidth, Network failure rate, NS2**

I. INTRODUCTION

Dynamic WSNs are adapted in monitoring applications, battle field surveillance, health care, vehicle status monitoring, dairy cattle, health monitoring and traffic flow, as dynamic WSN provides wider network coverage and accurate services than static WSNs. As sensory devices are at high risk of malicious attacks due to careless operative environments and lapses of connectivity in wireless communication, security is the main factor to be considered. Node authentication, data integrity and confidentiality are the security requirements during node mobility [1]. Sensor networks comprises of small autonomous devices. Each of that small device is called as sensor node. Each node is battery powered and integrated with sensors, short range radio communication and data processing .In the deployment region sensor nodes spread randomly and collect sensor data [2].Security is the main factor to be considered when sensor networks are deployed in hostile environment, as they are vulnerable to many attacks like malicious attacks. An adversary can compromise to other nodes and leak the information, so here in this type of attacks, communication should be encrypted to provide security.

Symmetric key encryption is suited for sensor nodes who have limited energy and processing capability. CL-EKM (certificate less effective key management) scheme does not provide support for node mobility, not resilient against attacks and it is not secure. In asymmetric key encryption method public key cryptography (PKC) is used such as elliptic curve cryptography (ECC) or ID-PKC (Identity based public Key cryptography), as it simplifies key establishment and data authentication between sensory nodes. PKC based schemes are more reliable and scalable but its computational cost are more. ECC based schemes does not provide more security, they are vulnerable to attacks and gets easily compromised. ECC based scheme are not practical for large scale WSN applications, as they suffer from certificate management overhead. In CL-EKM the user's private key is a combination of a partial private key generated by a key generation center and the users own secret value. From CL-HSC (certificate less hybrid singryption scheme), node authentication and pair wise key establishment between nodes can be done. Due to CL-HSC, sharing can be efficiently done without pairing and exchanging of certificates.CL-EKM is more reliable and scalable and is not vulnerable to attacks.

The problem with key management problem is key agreement problem and it has types: the trusted server scheme, the self-enforcing scheme and the key pre-distribution scheme. In trusted server scheme, key agreement between the nodes is done depending on trusted server. The self-enforcing scheme uses public key certificates which depend on asymmetric cryptography. In pre distribution, information about key is distributed prior to deployment among all sensor nodes. Keys can be decided prior to network deployment if nodes are in the same neighborhood. It is impossible to get to know about the neighbor nodes because of the randomness of node deployment .A best solution is to provide master secret key to all nodes. To obtain new pair wise key and to achieve key agreement, global master secret key can be used. The security of the entire network destroys if anyone of the node also gets compromised. Storing the master secret key increases the cost and energy consumption also gets increased. In random key pre distribution each sensor node receives a random subset of keys from a large key pool [2].

Communication and computational resources divides the network into clusters and cluster gathers all the data. Here amount of data that is transmitted from cluster to base station is reduced, by consuming less resource. Cluster sensor network is divided into homogeneous and heterogeneous sensor network. In homogeneous network, battery energy and

hardware complexity are identical. In static clustering in homogeneous network, Cluster head nodes will be over loaded to the base station with long range transmission in addition to the data aggregation and protocol co-ordination. As a result energy resources are consumed by the cluster head before other nodes. In heterogeneous network, different levels of battery energy and functionality are used for two or more different types of nodes. In a network ,total cost of hardware can be minimized and also providing longer life span by using cluster nodes or H-sensors that have extra battery energy, complex hardware and additional functionalities keeping rest nodes simple.[3]

When networks are to be deployed in hostile environments, such as military environment, security and privacy are the important issues. Robust key management is required to function properly for most available data security. But due to resource constraint key agreement establishment is not easy task in WSN. Probabilistic key pre-distribution is a key management scheme for WSNs. The probability of each sensor sharing at least one key with a neighbor sensor be high, to guarantee secure connectivity in the network between nodes. High key sharing probability means that each node requires large key space to store large number of keys. In this scheme sensor node selects key from key pool. Key pool should be large to achieve high key sharing probability.[3]

WSN has impact on improving and developing the telecommunication field beyond from transmission wire to the radio communication, thereby increasing the growth.WSN is nothing but group of nodes which are organized into cooperative network. The major challenge in WSN is image transfer which is related to its storage , representation an transmission. Due to restricted computational power, battery constraint and limited storage capacity and limited bandwidth, image transmission has become huge challenge. Wavelet scheme is efficient and it minimizes energy consumption required for wireless communication and it requires minimum bandwidth and also it meets network image quality. In Discrete wavelet transform, energy computation can be reduced by maintaining image quality by using image compression scheme. In this scheme transmission delay can be reduced and better compression ration can be achieved.[4]

Spatial distributed devices comprise WSN to monitor environmental conditions. Applications such as military and battlefield motivate development of WSN. Nowadays WSN have wide variety of application in the areas like healthcare, home automation etc.

In the below figure, data which is collected by sensors is transmitted to base station or sink which is of high processing capability and energy. To extract important information data sent by sensors will be collected and stored. The challenge in image transfer is to process and transmit huge amount of data. This puts demand on bandwidth as well as battery resources.

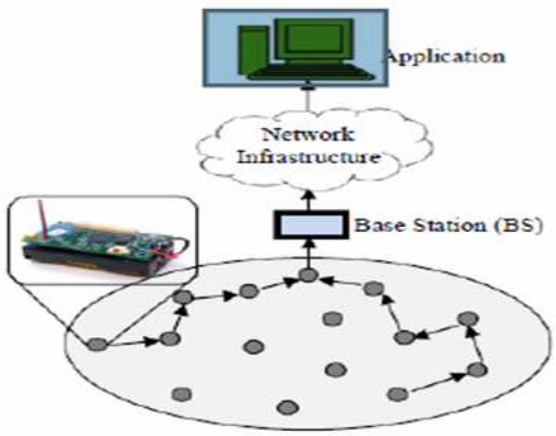


Fig : Wireless sensor network

To consume less energy images are compressed. By implementing image compression algorithm, image transmission improvement can be done over WSN, thereby reducing the number of bits which represents image by removing the spectral and spatial redundancies by reducing energy. Sharing of computation load can be done by distributed image compression. Individual node cannot possess large computational power to suppress large image data to meet requirements, this is not possible.[4]

Bandwidth and energy requirement is needed to transmit huge amount of data for image transfer in WSNs that cannot be completed by restricted power, limited battery technologies and limited storage. The main objective is to minimize energy and performance can be enhanced. [4]

WSN consists of sensors, processor, radio anbattery.WSN is formed from many sensor nodes in application area.WSN components are responsible for global warming. To detect and track submarines, acoustic sensors was deployed.[5].

WSN is collection of self contained, millimeter and electro mechanical devices. These tiny devices have computational ability, sensors, wireless transmitter and receiver and power supply. Large number of nodes spans geographical area. Distributed systems provide communication mechanism.[6]

Existing protocols are unable to access with large size of keys and also it increases overhead. In this project, Digital signature based key management protocol for secure data transfer in dynamic WSN is proposed. It is one of the most significant security services provided by cryptography in asymmetric key management. It minimizes overhead by increasing security and also minimizes energy consumption. This protocol is implemented in Network Simulator-2(NS2).A security analysis of the proposed scheme is effective in reducing Energy consumption, false data injection rate and Node failure rate.

The paper is organized as follows, section 2 describes literature survey. Methodology is described in section 3, followed by Hardware and software requirements in section 4.Results and discussion is explained in section 5.

II. LITERATURE SURVEY

This section describes the various literatures on providing reliability and security in wireless sensor networks.

"Secure Data Aggregation in Wireless Sensor Networks"

In many sensor applications, data which is collected from each node is sent to base station which usually takes much time to transfer the data individually. So now to reduce energy consumption data aggregation technique is introduced, here the aggregated data from the sensor nodes are sent to the base station. The earlier existing algorithms do not include security. So they were vulnerable to wide variety of attack. By this if any intruder occurs these nodes by aggregation removes all the false data and further aggregate to the base station.

"A Survey of Attack and Defense Techniques for Reputation Systems"

Reputation systems is a process through which many parties can express the trust between one another. These systems help to generate an exact correction in the face of without equal community size, while providing unusual features and flexibility to malicious attacks. They mainly look on attacks and defense mechanisms in reputation systems. Hence they analyze several landmark systems, characterizing their individual strengths and weaknesses.

There main work is

1) Which drawing components are more unsafe.

2) What are the most accurate protection mechanisms.

3) How these protection mechanisms can be combined into existing or future reputation systems to make them flexible to attacks.

"An Efficient Approach For Secure Data Aggregation Technique For WSN In The Presence Of Security Attacks"

In many sensor applications, data which is collected from each node is sent to base station which usually takes much time to transfer the data individually. So now to reduce energy consumption data aggregation technique is introduced, here the aggregated data from the sensor nodes are sent to the base station. The earlier existing algorithms do not include security. So they were vulnerable to wide variety of attack. So they have introduced secured data aggregation which provides security for data aggregation from attackers, This process can also enhance the strong and exact information. Iterative filtering algorithm is one algorithm to perform secure data aggregation and also provides security to whole network.

"Data Aggregation Techniques in Wireless Sensor Network Survey"

Data aggregation is a process of collecting ,grouping and aggregating the useful information from nodes to the base station, here it mainly deals with the energy consumption, as by doing this energy is reduced. This is very important technique in wireless sensor network. It plays main role in energy consumption, so that network lifetime also reduces. In this paper it is based on routing protocols and algorithms. It mainly aims at eliminating redundant data transmission. It also solves the overlap problems.

''Effective Key Management in Dynamic Wireless Sensor Networks'' :

This paper propose a protocol for secure data transmission in dynamic wireless sensor network and defines the various types of attack that may occur in the communication path ,The proposed technique also ensures the minimum impact of compromised node on other communication links.

''The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks'':

This paper explains about the simplicity and efficiency of the dynamic source routing protocol because of its self organizing and self configuring behavior without any need of infrastructure, it also explains the overall mechanism of DSR algorithm as well as it shows the operation of DSR in some of simulation and compare the results for the protocol.

''Comparative Study of AODV, DSDV and DSR Routing Protocols in Wireless Sensor Network Using NS-2 Simulator'':

Based on performance and various other factors there are number of routing protocols for WSN , and this papers compares the popular AODV, DSDV and DSR algorithms to analyze the result for throughput, End to End delay, Packet delivery ratio.

''Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes''

This Paper suggest a novel solution to defend the OLSR protocol from node isolation attack by employing the same tactics used by the attack itself. Through extensive experimentation this Paper demonstrate that 1) the proposed protection prevents more than 95% of attacks, and 2) the overhead required drastically decreases as the network size increases until it is non-discernable.

Lastly, It suggest that this type of solution can be extended to other similar DOS attacks on OLSR.

"Evaluation and Mitigation of DoS attack using behavior Anomaly Detection approach using NS-3 "

This article is going to evaluate scheme in two popular routing protocols of MANET i.e. OLSR and DSR presents the results and discussion about proposed scheme effectiveness. Results show that the performance of proposed method is better than other existing method. Future work of the proposed method will focus on enhancing it capability to apply on WiMax and 4G communication system to detect other types of attack as well and we will also plan it to test it on other routing protocols. Proposed approach has been tested under NS-3.14 MATLAB tools.

"Mitigating DDoS Attacks using Protection Nodes in Mobile Ad Hoc Networks "

In this paper, a novel approach to alleviate the impact of DoS or DDoS attacks in MANETs based on AODV (Ad hoc On demand Distance Vector) routing protocol. The method, which is named Protection Nodebased Strategy, is based on two fundamental assumptions: first, the attacker is not aimless; and second, the MANETs adopt a hierarchical architecture, and the nodes are classified into different levels according to their importance. This scheme is suitable to be applied in environments where lower level nodes are willing to protect higher level nodes.

"DDoS Attack and Defense Scheme in Wireless Ad hoc Networks "

This Paper uses the medium access control (MAC) layer information to detect the attackers. The status values from MAC layer that can be used for detection are Frequency of receiving RTS/CTS packets, Frequency of sensing a busy

channel and the number of RTS/DATA retransmissions. Once the attackers are identified, all the packets from those nodes will be blocked. The network resources are made available to the legitimate users.

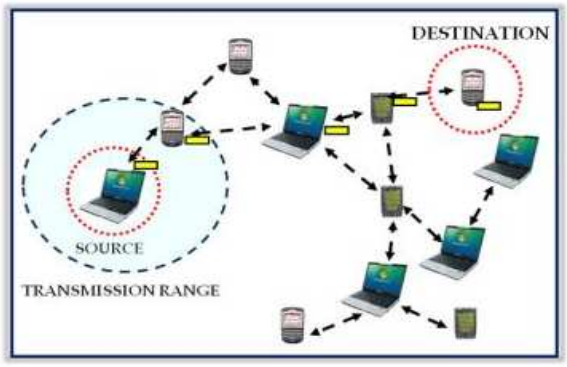
"A Review for Detection of Distributed DOS Attack in MANET "

This paper focuses on mobile ad hoc networks -routing vulnerability and analyzes the network performance under Distributed Denial of Service MANETs. The resistive schemes against these attacks were proposed for ad hoc on demand Distance Vector (AODV) routing protocol and the effectiveness of the schemes is valid using NS2 simulations.

- METHODOLOGY

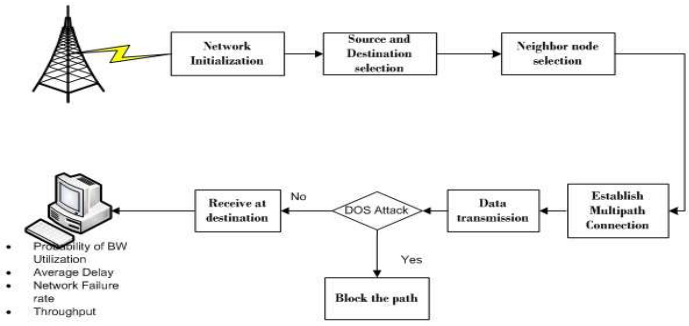
Aim is to prevent or detect malicious nodes launching black-hole attacks as well as denial of service attack is a challenge. This project attempts to resolve this issue byapplying algorithms in order to provide security as well as reliability.

The final result are based on following parameters: Average Delay, Probability of bandwidth utilization, Network failure rate,Throughput.



In this paper we review a specific DOS attack called node isolation attack and propose a new mitigation method. Our solution called Denial Contradictions with Fictitious Node Mechanism (DCFM) relies on the internal knowledge acquired by each node during routine routing, and augmentation of virtual (fictitious) nodes.Moreover, DCFM utilizes the same techniques used by the attack in order to prevent it. The overhead of the additional virtual nodes diminishes as network size increases, which is consistent with general claim that OLSR functions best on large networks.

- Advantages of Proposed System: Prevent a node isolation attack in which the attacker manipulates the victim into appointing the attacker as a sole MPR, giving the attacker control over the communication channel. We further strengthened the attack by giving the attacker the ability to follow the victim around.
- Architectural Diagram:



In the above block diagram, network deployment is done to initialize all nodes. Before network deployment, all the parameters will be generated by the base station (BS) and BS registers node mentioning it in member list. Once network deployment is done, all the nodes starts to advertise by sending broadcast message with its neighbors to trigger pair wise key setup. The message consists of public key and identifier. Pair wise encryption key can be derived by setting pair wise master key. To encrypt the data pair wise encryption data can be used.

- Distance and energy between all nodes will be calculated. Neighbour nodes will be discovered by sending the beacon messages. After neighbor node discovery, key is distributed to all the nodes. Public key is distributed to everyone which will be used to verify the signature. Private Key is known to user which will be kept secret and it is used to generate the key.

Through multipath establishment data will be transmitted through different paths. If intruder attacks any of the path means, that path will be blocked and data will be transmitted through other path.Distance between each node can be calculated using the formula,

$$D=\sqrt{(y_2-y_1)^2+(x_2-x_1)^2}$$

Where,x2, x1-x axis position of node , y2, y1-y axis position of node In key distribution mechanism, DSA (digital signature algorithm) is used. Digital signatures (DS) are used to increase the security. DS verifies the sender of documents identity. .A digital signature is represented as a string of binary digits. Private Key generates signature .Digital signatures are used to detect unauthorized modifications to data. Digital signature algorithms can be used in e-mails electronic funds transfer, electronic data interchange, software distribution, data storage, to assure the integrity and originality of data. Here hash function is used to generate the key. It compresses the data and compressed data is called message digest. This message digest produces digitally signed message.

- At the receiver side also hash function is used for verification purposes. Message which is less than 264 bits as input, message digest will be of 160 bits. As message digest is of small size compared to message, efficiency can be improved by signing the message digest [15].

III. DSA ALGORITHM:

- DSA algorithm steps:
- DSA parameters:
- P=prime number of length 2L-1<p<2L for 512≤L≤1024,

L= (512, 576, 640, 704, 768, 832, 896, 960, 1024)

- •q = a prime divisor of p-1, where 2159 < q < 2160
- 1) Choose sequence of 160 bits as seed, g is the length of that seed.
- 2) Formulate
- U=SHA-1[seed] XOR SHA-1[(seed+1) mod2g]
- 3) Formation of q from u, q=U 0R 2159 OR 1.
- 4) Test q is prime or not by primality testing algorithm.
- 5) If q is not prime, go to step 1
- 6) Let counter=0 and offset=2
- 7) For k=0, 1, ...n, let
- Vk =SHA-1[(seed+offset+k) mod 2g]
- 8) Let W be the integer,
- W=V0+V1*2160+.....+Vn-1*2(n-1)*160+ (Vnmod2b)*2n*160
- And let X=W+2L-1.note that 0≤W<2L-1 and hence
- 2L-1≤X<2L
- 9) Let c=Xmod2q and set p=X-((-1))
- 10) If p<2L-1 then go to step 13
- 11) Test whether p is prime or not.
- 12) If p is prime then go to step 15.
- 13) Let counter=counter+1 and offset=offset+n+1.
- 14) If counter≥212=4096 then go to step 1 else if counter<4096 then go to step 7.
- 15) For proper generation of p and q, same seed value and counter will be used.

Explanation of algorithm steps:

Choose length L=512,576,640,……1024.Select prime number, p between the length 2L-1 and 2L .Length is multiple of 64.choose q, a prime divisor of p-1,where q lies between 2^{159} and 2^{160}.Choose sequence of 160 bits as seed, g is the length of that seed. Compute, U=SHA-1[seed] XOR SHA-1[(seed+1) mod2g].SHA is a secure hash function and string of bits form seed. Form q from U, q=U or 2^{159} or 1.By using primary test algorithm, we should test q is prime or not. If q is not prime, go back to step 1.Counter will be initialized to zero an offset taken for 2 ,i.e. counter=0 and offset=2.Find Vk =SHA-1[(seed+ offset +k) mod 2g] for k=0,1,2……..n. Let W be the integer, w=V0+V1*2160+.....+Vn-1*2(n-1)*160+ (Vnmod2b)*2n*160.And let X=W+2L-1, where W lies between 0 and 2L-1 and hence 2L-1≤X<2L. Let c=Xmod2q and set p=X-((-1)).If p<2L-1, then go back to step 13 and check whether p is prime or not by using primary testing algorithm. If p is prime go back to step 15.Let counter=counter+1 and offset=offset+n+1. If counter≥212=4096 then go to step 1 else if counter<4096 then go to step 7.For proper generation of p and q, same seed value and counter will be used.

P, q and g are the parameters which made public. Private key. X and public key Y are the keys users have. X and k are used for generation of signature and must be kept secret. For each signature, K will be randomly or pseudo randomly generated.

The message M is pair of numbers r and scan be calculated using,

$r= (g^k \bmod p) \bmod q$

$s = (k^{-1}(SHA (M) +xr)) \bmod q$

SHA (M) is 160 bit string, is converted to integer according to SHS standard. For verification purpose, signature is used.[15]

A. *VERIFICATION*

The receiver must know the parameters p, q, g and senders public key y before getting digitally signed message. Consider $m^{|}$, $r^{|}$ and $s^{|}$ which are received version of m r and s. for verifying signature, Verifying program should check conditions like $0<r^{|}<q$ and $0<s^{|}<q$, if anyone of the condition fails then that particular signature will be rejected .If both the conditions are satisfied then we will compute,

$W= (s^{|})^{-1} \bmod q$

$U1= ((SHA (M^{|})) w) \bmod q$

$U2= ((r^{|}) w) \bmod q$

$V= (((g)^{n1}(y)^{n2}) \bmod p) \bmod q$

If $V=r^{|}$ then the obtained signature is valid otherwise message has been changed.

IV. DSR PROTOCOL

In mobile networks for communication among nodes there is no need for any fixed infrastructure as these nodes are connected to each other via wireless connections and exchange their data with the help of relay nodes with the help of discovery of routes for this various types of protocols are exist some of the very popular routing protocols are AODV, DSR and DSDV protocols for efficient and in time delivery of packets.

These protocols are characterize into two model:

Proactive and Active Protocol

DSDV is Proactive which means that it is a Table driven model as it has to maintain a routing table before forwarding packets so that all nodes which establishes route should have prior knowledge about all nodes which follows the path. While AODV AND DSR are active as it is a on demand Routing protocol and no need to maintain routing table.

Here our idea is to use DSR algorithm to establish route because of its features like it reduces bandwidth overhead, less power consumption as well as no need to maintain updates about routes , The only effort is to identify link failures .

A. *Working Principal of Dynamic Source Routing Protocol:*

DSR is one of a simple protocol designed remarkably for multi hop network because it is self organizing and self configuring ,hence no need for infrastructure. DSR focuses on regular updating of its route cache in order to get easy routes so that it can forward the packets from the newly establish route, As there is no concept for routing table so to make the packets know which path has to follow , route information is attached in each packet's header to reach its destination node. Hence DSR follows two mechanism ROUTE DISCOVERY and ROUTE MAINTENANCE.

B. *ROUTE DISCOVERY:*

For establishing the route source node will broadcast Route Request message in the network, after getting the request message all the neighbor node add its address and

rebroadcast it till message reach to destination node this way route is discovered between source and destination,

There is one assumption that has to be followed ie in case when the route is very new which means no previous transmission occurred and if path is already existed then nodes will not broadcast Route Request in the network. This planning is done with the help of cache as all the nodes maintain its route cache, and it also helps in reducing memory overhead sending request to the destination with the full description about route instead of broadcasting and then destination will send Route Reply to source.

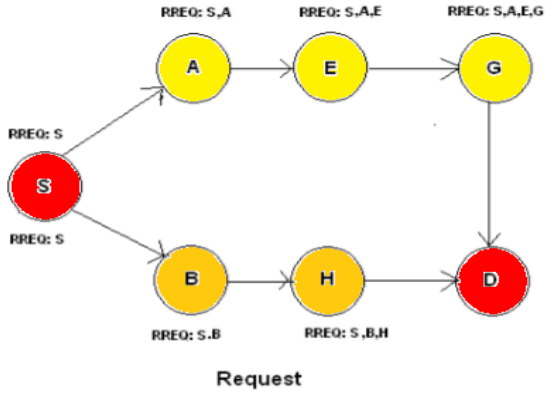


Fig : Route Request Mechanism

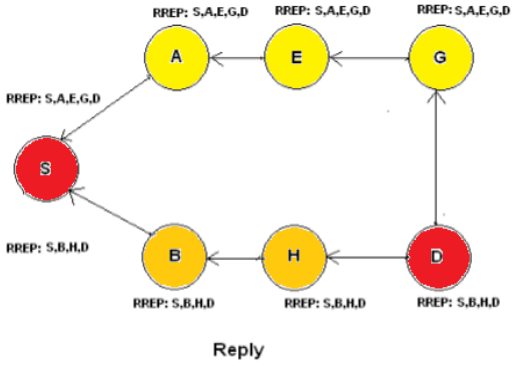


Fig: Route Reply Mechanism

C. ROUTE MAINTENANCE:

While forwarding the packets from the source node, all the relay nodes which directs to the destination node has to give conformation receipt that packet is forwarded successfully or else packet is retransmitted until node will get conformation receipt. This conformation receipt can be of many form such as link level acknowledgement defined by 802.11 standard or passive acknowledgement, suppose 3 relay nodes say B,C,D are present in between source node and destination node so that B conforms receipt over C by overhearing that C forwards packets to node D and the another technique is DSR-specific software acknowledgement in this form the node which is forwarding the packets set a bit in the header to request acknowledgement should be given by the next intermediate node, basically this acknowledgement is sent directly to the sending node but if in case route is unidirectional then acknowledgement has to be sent via relay nodes.

During propagation if any relay node is transmitting packets several times and it is not getting acknowledgement in that case node will send ROUTE ERROR message to the sending node so that it will stop forwarding the packet and blocks that path and search in its cache for another route , incase route is not found in cache it will again broadcast ROUTE REQUEST message in the network to establish new route.

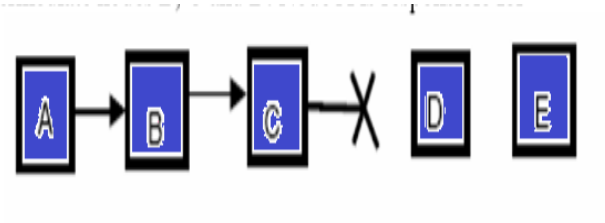


Fig : Path Disconnected Between Node C and D.

D. Software requirement:

HARDWARE REQUIREMENTS

- SYSTEM : Pentium IV 2.4 GHz
- HARD DISK : 40 GB
- MONITOR : 15 VGA color
- MOUSE: Logitech.
- RAM : 256 MB
- KEYBOARD: 110 keys enhanced.

E. SOFTWARE REQUIREMENTS

- OPERATING SYSTEM:Ubuntu 12.04.
- IMPLEMENTATION:NS2
- NS2 VERSION:NS2.34
- FRONT END:OTCL (Object Oriented Tool Command Language)
- BACK END:C++
- PLOTTING: X graph

Network Simulator (NS2.33):NS2 is a discrete event driven simulator developed at UC Berkeley, supports networking research for designing new protocols or comparison of protocols. It is an open source simulator compatible with FreeBSD, Linux, Solaris and Mac OS.

Structure of NS2:NS2 is an object oriented simulator since it is built using object oriented methods in C++ and OTCL(Object oriented tool command language) interpreter. In NS2 TCL language is written for frontend whereas backend is written in c++ and when it is compiled trace file and nam file is created which shows the movement of nodes, packet sending , no of relay node between two nodes, connection type ,topology, packet type, initial energy, network type etc

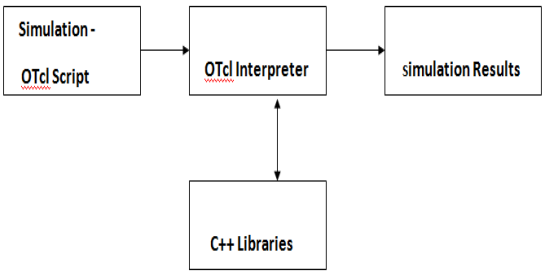


Fig : Block Diagram of user view in NS2

It supports 2 languages because:

C++ supports simulation of any protocol system programming language is required as it manipulates bytes, process packets and for this run time speed is very important and turn around time should be slower for simulation, fixing and finding bugs or recompile or rerun.Whereas TCL is helpful because it involves slightly varying parameters or configurations and quickly explores various scenarios for which iteration time is important and runtime does not matter so much.Hence NS2 needs both the languages.

V. CONCLUSION AND FUTURE WORK:

In this paper, we proposed a digital signature based protocol for secure data communication in dynamic WSNs. Digital signature ensures efficient communication and updates node movements. Our proposed system increases data security and confidentiality .Proposed system reduces Energy consumption, throughput and average delay and probability of bandwidth utilization, with the increase in number of nodes. As future work, we need to work with node mobility and multiple parameters which degrade the network performance, also proposed technique used DSR routing protocol to avoid over all traffic also decreases the network delay due to dynamic path discovery scheme.

REFERENCES

[1] Seung-Hyun Seo, Member, IEEE, Jongho Won, Student Member, IEEE, Salmin Sultana, Member, IEEE, and Elisa Bertino, Fellow, “Effective Key Management in Dynamic Wireless Sensor Networks”, IEEE1556-6013 (c) 2013 IEEE

[2] Wenliang Du, Member, IEEE, Jing Deng, Member, IEEE, Yunghsiang S. Han, Member, IEEE, and Pramod K. Varshney, Fellow, IEEE, A Key Predistribution Scheme for Sensor Networks Using Deployment Knowledge IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 3, NO. 1, JANUARY-MARCH 2006.

[3] Sk.Md.Mizanur Rahman, Khalil El-Khatib,“Private key agreement and secure communication for heterogeneous sensor networks”, 0743-7315/$ 2010 Elsevier Inc.