Behaviour based Detection of Worm Hole Attack and for Secure Transmission use AES in MANET

Khushboo Shrivastava[1], Vikas Sejwar[2]
[1, 2] Department of CSE/IT
[1, 2] Madhav Institute of Technology and Science, Gwalior, Madhya Pradesh

Abstract- *mobile ad-hoc network is growing field of research there are lots of work done regarding in this field, attacks easily deploy in this network due its property and flexibility worm hole attack one of the crucial attack of this network because identify two malicious nodes is very difficult. In this paper we study about network, cryptographic approaches and various technique to prevent this network by worm hole attack. We proposed a behavior based detection technique and for preventing we send data by using AES technique so that we safe our network from passive attacks too. Implementation of our work done on ns-2.35 and for novelty of our work we give various result by which we proof that using this approach quality of service of our network is improve .*

Keywords- MANET; AES; pdr; IDS;

I. INTRODUCTION

Popularity of an Ad hoc networking increases these days due to simply join and leave of nodes in the network. It permits to devices to preserve network connections. Also Ad hoc network gained much more attention because of reduced cost, improved technology equated to wired networks. Several standards for wirelessly networks have arrived into existence so as to address the needs of both industrial and individual users. One of most common forms of WSN in exploit nowadays is MANETs. The applications for MANETs are ranging from large-scale to small scale networks. MANET is Frameless network involving of self-designing and adopting mobility nodes connected thru wirelessly links in which Nodes depend on each other to store and pass ahead the packet. All device is consisting of trans receiver, to communicate with other nodes in its geographic area. Multihop communication is nothing but mutual interaction or cooperation of every other node in path or route in the network is required to reach a packet to a node that is out of its geographic area. Therefore, each and each node at same time must act as host and router too. Due to solitary characteristics of MANETs which is comparatively immune to attacks than wired network prevention techniques alone will not stand to provide security, as they were planned for a set of known attacks. They cannot accustomed prevent new attacks that are planned for bypassing the current security measures. Therefore, detection must be added as other criticism before an attacker may break the system. Switches, gateways or routers are the devices through which IDS may be implemented easily in wired n/w but it is not the case for MANETs which cannot satisfy such condition as it does not have such devices. Due to MANETs Vulnerabilities both legal and illegal users can access it. Moreover boundary of separation is required between normal activities also abnormal or unusual activities in a mobile n/w. Thus, existing wired IDS techniques cannot be applied directly to MANETs, So many IDS have been suggested for MANETs, which will be explained in next section [1].

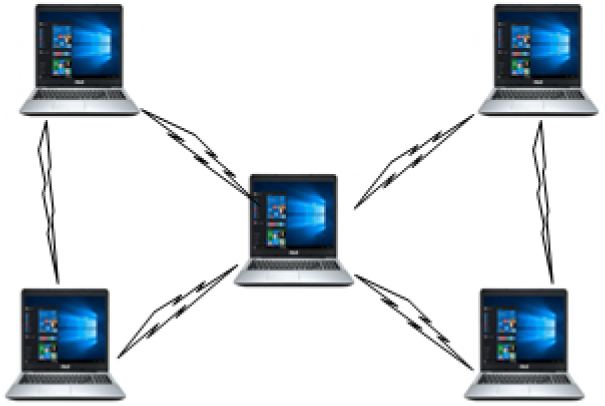

Fig 1 MANET

II. AES

AES stand for “advanced encryption standard”. It is iterated block cipher using a fixed block size of 128 and variable key length i.e. key sizes 256 and 192 depend on number of rounds. Neighboring finding/discovery protocol helps to communicate amid neighboring nodes in the mobility IPV6 atmosphere and can be provided with secures function by including the RSA signature options and CGA 149 parameters option but, the SEND protocol unable to give confidentiality of ND Massage. To provide confidentiality of transfer protocol AES algorithm may be used with symmetric key without certification authority or any security infrastructure. Every round contains various processing steps, together with an encryption key.

The AES is a symmetric key decryption and encryption algorithm that used for converting cipher text to plain-text and vice-versa. Since the equal key or master key is used, the must be reserved secret or with trusted 3rd party, because compromise of this key would mean compromise to the data.

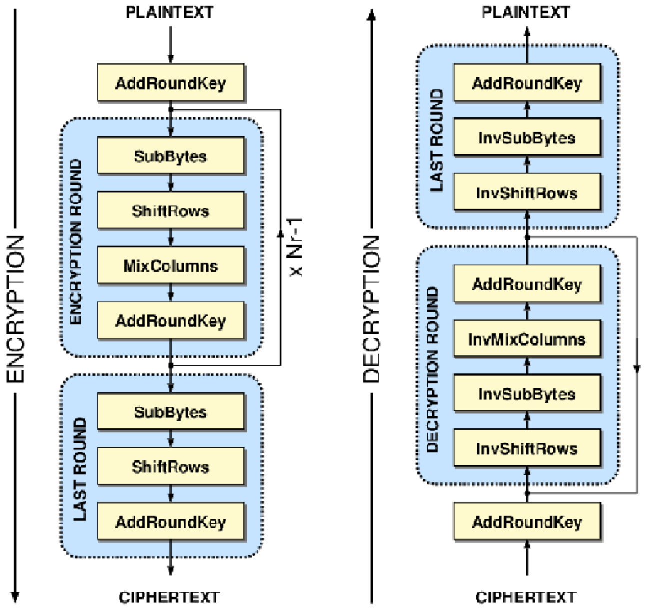

Fig. 2 Architecture of AES

1) Key Expansion round keys are derived from cipher key exploiting the Rijndael's key schedule. To make round keys for all round, AES algorithm exploit a key process. If the numbers of rounds are Nr, the key expansion routine makes Nr+! 128-bit round keys from one sole 128-bit cipher key [2].

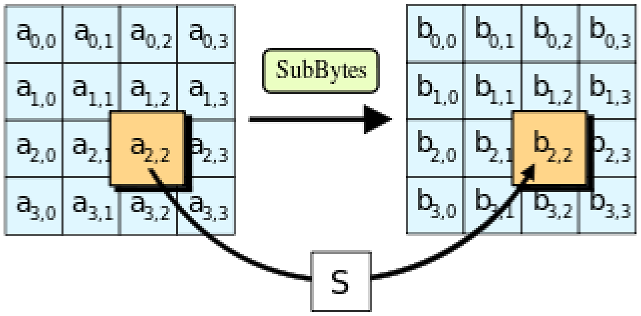

Fig. 3 Sub Bytes Operation

2) Initial Round

a) Add Round Key: In this step, all byte is groups with round key exploiting bitwise XOR.

b) Rounds

- Sub Bytes are the main building block of AES is regarding side-channel aspect. This is nonlinear substitution step where byte is substituted according to lookup table as illustrate in Figure 2.

- Shift Rows is transposition phase that all row of phase is shifted cyclically a certain amount of steps.

- Mix Columns is mixing operation that operates on columns of state, byte value is changed based on the values of all bytes in the column by multiplying the state in GF (28). Figure 4 illustrates the Mix columns operation, using the polynomial shown in following equation:

M(x) =x8 +X4 +x3 +x + 1

3) Add Round Key: This is the last step of the rounds of encryption process. In this step XOR operation take place column-wise.

4) Last Round

- Sub Bytes
- Shift Rows
- Add Round Key [2].

III. LITERATURE SURVEY

[3] Mona Sabry (2015) et al presented the DNA based implementation and design to "Advanced Encryption Standard" [AES]. We make algorithm using all specifications on DNA basis instead of bits. This aims at proving the possibility of building such a complex system on DNA basis in a way of making it a suitable candidate for implementation in biological environment or on DNA computers. Our algorithm kept the same security strength and robustness of the standard algorithm.

[4] A.P. ANUSHA NAIDU (2015) et al presented the FPGA based implementation of 128-bit AES exploiting completely pipelined architecture. Suggested architecture may deliver higher throughput at both decryption and encryption operations. Xilinx ISE design suite 13.1 is exploited for Spartan-3 and design for implementation.

[5] Jishamol T. K (2013) et al presented that a low region design and low power for AES depend on an 8-bit data path. This has most important power-area-latency performance progresses over normal 128-bit data path AES. Such improvements are attained thru use of resource sharing, simple compact memory architecture, Low Resource Mix Column Circuit, minimizing memory transfers and avoiding needless switching activity. As well as performance needs of AES, this must be reliable against transient or permanent internal faults. Faults which accidently arise in h/w implementations of AES

can cause erroneous output. At end of plan, Paper presents parity-depend fault detection design for high performance AES implementations.

[6] Akash Kumar Mandal(2012) et al prsented that two most broadly exploited symmetric encryption methods i.e. DES and AES have been executed with MATLAB software. After the implementation, these techniques are compared on some points. Points are avalanche outcome because of one bit variation in key keeping memory required, plaintext constant for implementation as well as simulation time required for encryption.

[7] Charles Bouillaguet (2012) et al presented that dissimilar method, restricting data available to adversary to few ciphertext/plaintext pairs. We argue which idea of such attacks improves understanding of security of block ciphers of another cryptographic primitive based on block ciphers.

[8] Jishamol T. K (2013) et al presented that a low region and low power design for AES based on an 8-bit data path. This has important power-area-latency performance increases over normal 128-bit data path AES. Such improvements are attained thru use of resource sharing, simple compact memory architecture, Low Resource MixColumn Circuit, minimizing memory transfers and avoiding needless switching activity. Along with performance requirements of AES, it should be reliable against permanent or transient internal faults. At end of design, Paper presents parity-depend fault detection design for high performance AES implementations.

III. PROBLEM STATEMENT

MANET is easily to diffuse and thru exploiting MANET communication going to be easily. Due its flexibility and infrastructure it easily threatens by attack. Worm hole attack one of the crucial attack of MANET, in this attack two node create a tunnel and communicate to each other or drop the data or modify the data so that find out worm hole tunnel is tough.

In existing technique “Defending against Wormhole Attack in MANET” finding the wormhole tunnel author apply HCF based technique in which node encrypted the route information by using hash value. Then compare the RREQ value of nodes if any mismatch found network nodes declare that node as malicious nodes but it’s not a right way to find out malicious nodes because topology of network changes frequently so this value is changed.

In our propose work for finding of worm hole attack we apply behavior based technique and for secure transmission we use AES technique “in MANET, hybrid method for defending wormhole attack”.

IV. PROPOSE WORK

Mobile ad-hoc network is most popular due its infrastructure and mobility, MANET is gaining popularity due its applications and usability. This network is easily effected by attacks and worm hole attack is one of the crucial attack for this network. For prevention this we apply behavior based detection of nodes in which first we check RREQ or RREP of nodes than we check neighbor information of nodes, at the time of packet send when source node ask neighbor nodes and any mismatch found it check nodes RREQ or RREP if there values below thresh hold than nodes block these nodes and search another secure path this technique work when active attacks are perform but in case of passive attacks this technique does not perform well for secure our network we send our data using AES algorithm.

```
Step1: initialize network

Step2: check neighbours

Step3: update neighbours table

Step4: send data

Step5: if(RREP not rcv){

Chk(neighbor){
Block these node                    // after mismatch found

Step6: encrypt data using AES

Step7: decrypt data using AES

Step8: exit.
```

AES algorithm

```
Step1: byte state [16]

Step2: state = in

Step3: AddRoundKey(state, round_key[0]);

Step4: for i = 1 to Nr-1

Step size 1

do
```

SubBytes(state);ShiftRows(state);MixColumns(state);

AddRoundKey(state, round_key[i]); end for SubBytes(state);

ShiftRows(state); AddRoundKey(state, round_key[Nr]); end

step5: exit

Simulation and result

Simulation of our work done on ns-2.35 where for routing we choose AODV protocol with AES security remaining parameter mention below.

Tool	Ns-2.35
Number of nodes	30
Mac	802_11
Antenna	Two ray ground
Buffer	Droptail
Stop	100ms

Packet delivery ratio: packet deliver ratio defines as numbers of packets receive by destination among sends packets.

PDR= (total receive packet/total send packet)*100

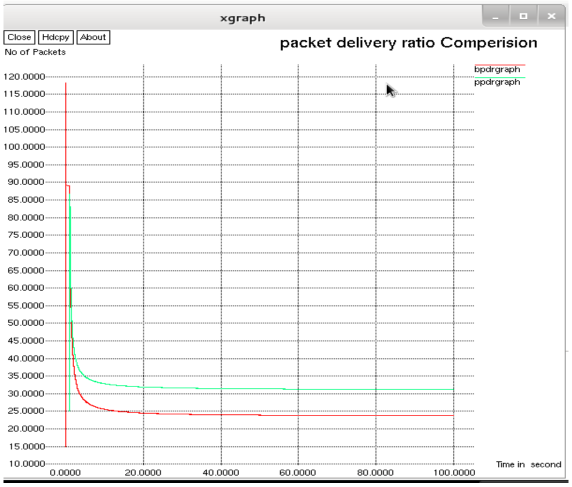

Fig: packet delivery

Above figure shows comparison between existing technique and propose work in which green line shows propose and red line represent existing technique, and this graph shows that propose perform better in above mention scenario

Throughput: throughput define as number of bits transfer per second over the band width

T = I/R

Where T is throughput, I is number of unit contain in a system, R is the process in which data deliver

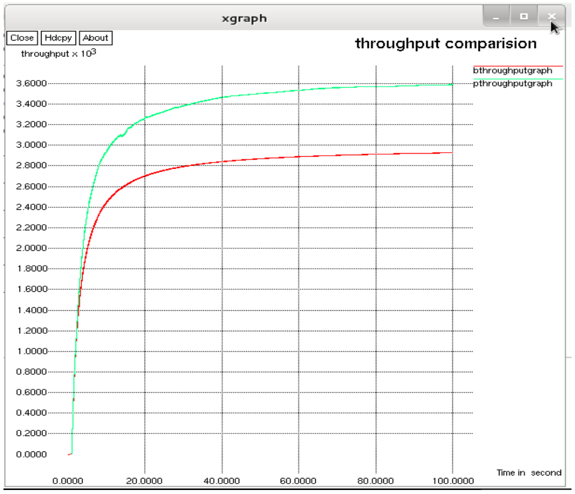

Figure: throughput

Above figure shows comparison between existing technique and propose work in which green line shows propose and red line represent existing technique, and this graph shows that propose perform better in above mention scenario.

Routing over head: routing overhead define as how many packets send for network information

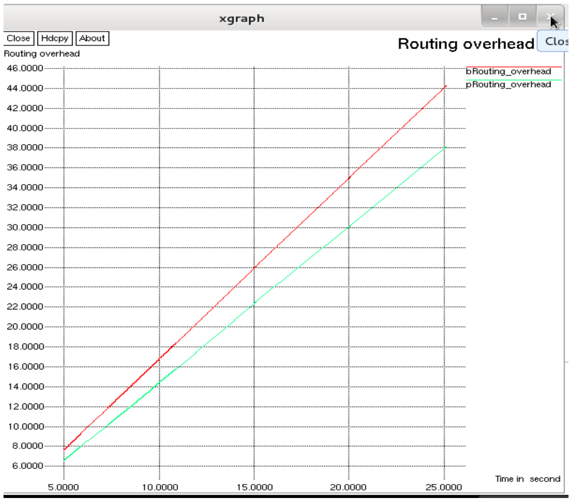

Figure: routing overhead

Above figure shows comparison between existing technique and propose work in which green line shows propose and red line represent existing technique, and this graph shows that propose perform better in above mention scenario.

Send packet: how many packets send for communication and data transfer.

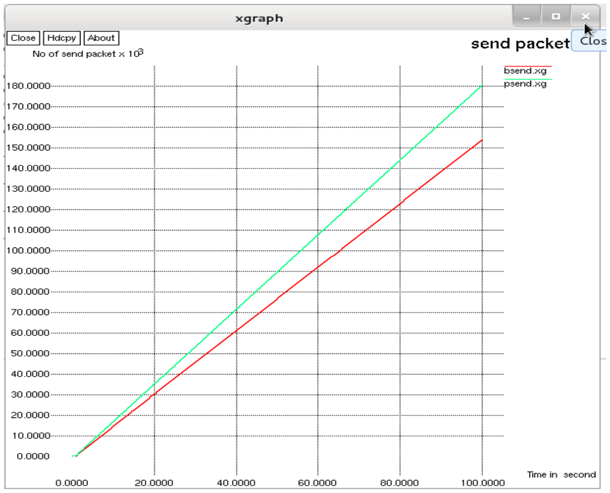

Figure: send packet

Above figure shows comparison between existing technique and propose work in which green line shows propose and red line represent existing technique, and this graph shows that propose perform better in above mention scenario.

Drop packet: packet drop define as number of packets drop in whole scenario.

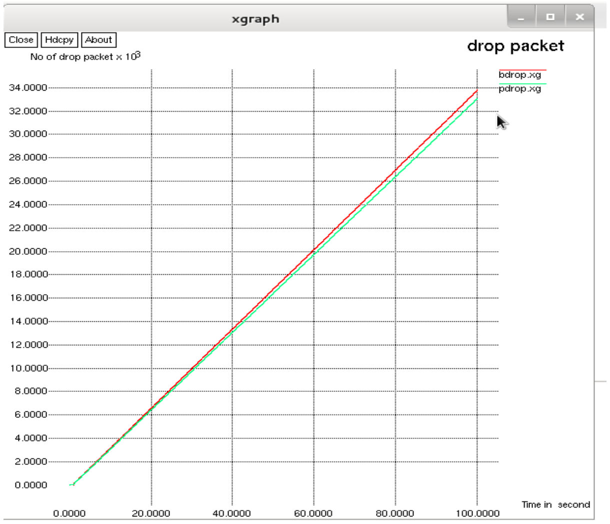

Figure: drop packet

Above figure shows comparison between existing technique and propose work in which green line shows propose and red line represent existing technique, and this graph shows that propose perform better in above mention scenario.

Receive packet: number of packets receive by nodes.

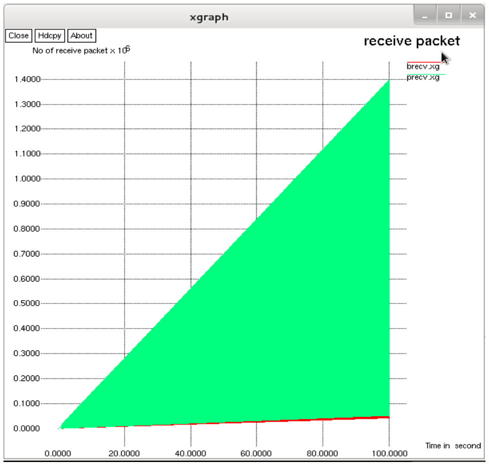

Figure: receive packets

Above figure shows comparison between existing technique and propose work in which green line shows propose and red line represent existing technique, and this graph shows that propose perform better in above mention scenario.

Forward packet: number of packet forward by intermediate nodes.

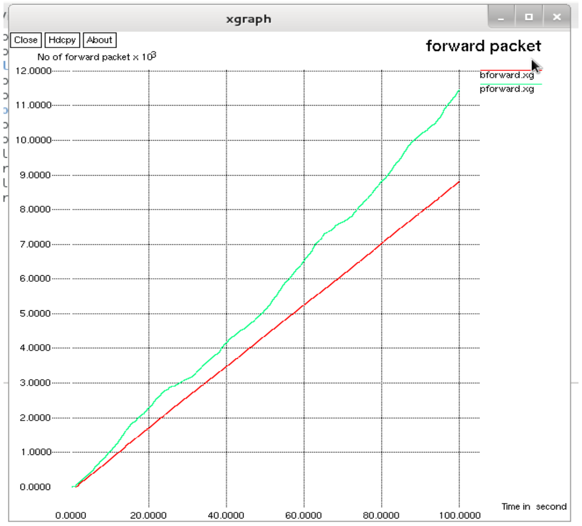

Figure: forward packet

Above figure shows comparison between existing technique and propose work in which green line shows propose and red line represent existing technique, and this graph shows that propose perform better in above mention scenario.

V. CONCLUSION

Mobile ad-hoc network is now growing field of research in this paper we study various technique and there problem by simulation result we conclude that our proposed technique performed better in compare to existing technique that mean propose technique provide better quality of service in network . our proposed technique also work for security. In future we apply light weighted cryptography so that performance also increase with respect to time.

REFERENCES

[1] Mrs. Rashmi K. Mahajan, Mr. Sanjay. M. Patil, "Protection Against Data Drop, An Enhanced Security Model of Authentication Protocol For Ad-Hoc N/w", 978-1-4799-7678-2/15/$31.00 ©2015 IEEE.

[2] Kavita T.Patil, Manoj E.Patil, "Improve the Security of CGA using Adjustable Key Block Cipher based AES, to Prevent Attack on AES in IPV6 over MANET", 2014 IEEE Global Conference on Wireless Computing and Networking (GCWCN).

[3] Mona Sabry, Mohamed Hashem, Taymoor Nazmy, Mohamed Essam Khalifa "Design of DNA-based Advanced Encryption Standard (AES)", 2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems.

[4] A.P. ANUSHA NAIDU, B. Prof (Mrs.) POORVI K. JOSHI," FPGA Implementation of Fully Pipelined Advanced Encryption Standard", 978-1-4 799-8081-9/15/$3l.00 © 2015 IEEE.

[5] Jishamol T. K, Mrs K. Rahimunnisa," Low Power and Low Area Design for Advanced Encryption Standard and Fault Detection Scheme for Secret", 978-1-4673-4866-9/13/$31.00 ©2013 IEEE.

[6] Akash Kumar Mandal, Chandra Parakash, Mrs. Archana Tiwari, "Performance Evaluation of Cryptographic Algorithms: DES and AES", 978-1-4673-1515-9/12/$31.00©2012IEEE.

[7] Charles Bouillaguet, Patrick Derbez, Orr Dunkelman, Pierre-Alain Fouque, Nathan Keller, and Vincent Rijmen," Low-Data Complexity AttacksonAES",0018-9448/$31.00 © 2012 IEEE.

[8] Jishamol T. K, Mrs K. Rahimunnisa, "Low Power and Low Area Design for Advanced Encryption Standard and Fault Detection Scheme for SecretCommunications", 978-1-4673-4866-9/13/$31.00 ©2013 IEEE.