International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 5, May - 2014

An Acknowledgement Based Ids With Random Key Generation For Manet

Prajeena Anilkumar
RVS college of Engineering and Technology,Coimbatore

Dr. S. Malathy M.E ,Ph.d
Head Of the Department
RVS college of Engineering and Technology,Coimbatore

Abstract-Mobile adhoc network(MANET), a flexible and infrastructure less network. It consist of many nodes which are free to move. Due to this dynamic nature of network, it is succeptible to various attacks.Drawbacks of previous intrusion detection schemes are on predistribution of keys. The requirement of distribution of predetermined key which is a major drawback ie key can be accesed by the malicious attacker and can forge the data which is encrypted using such key. Therefore the attacker can easily access the data sent by the source node.This paper mainly deals with the problem of false misbehavior report and attack caused by the distribution of predetermined key. The acknowledgement packet is to be authenticated such that the delivery of the packet is confirmed. Random key generation is used in order to avoid the attack on the distribution of predetermined key.Simulation tool used in this project is NS2.35 .Simulation result shows that the proposed scheme provide a reasonably good level of security than the existing system.This system is used in the military applications, banking etc.

Index Terms- **Diffie Hellman,RSA,digital signature, Adaptive,ACKnowledgement(AACK),TWOACKnowledgement(TWOACK),EAACK (Enhanced Adaptive ACKnowledgement)**

I INTRODUCTION

MANET is a flexible and infrastructureless network with scalability property in which, it has the capability to interface with many applications and has great adaptability to particular environment.It consists of various mobile nodes which are free to move in the network.Due to this dynamic nature of the network,it is susceptible to various attacks.MANETs are more vulnerable to attacks than wired networks.New approaches needed to be developed or else existing approaches needed to be adapted for the detection of attacks in MANET.There are various vulnerabilities of MANET.Resource unavailability is an issue faced by MANETs.Compromising of nodes and its restricted power supply are other problems faced. Some of the security goals of MANET are confidentiality, integrity and authentication. Due to the vulnerabilities of MANET,there is a need for the intrusion detection

schemes(IDS)[4][5].Intrusion is an action which the nodes compromise the above said security goals ie.integrity,confidentiality etc.IDS does its action in three steps ie.data collection,detection and response.Intrusion detection schemes can be categorized as anomaly based and misuse based.Anomaly means deviation from normal behavior and in case of misuse,it compares with a known attack ,hence does not detect a new attack.Some of the drawbacks which the intrusion detection systems dealing with are receiver collision,packet drop,limited transmission power and false misbehavior report.

Receiver collision occurs when a receiver received a packet simultaneously.An example for limited transmission power is shown in Figure 1 in which node B limits its transmission power so it is very strong to be overheard by node A after transmitting the packet 1 to node C , but too weak to reach node C because of transmission power can be reduced.

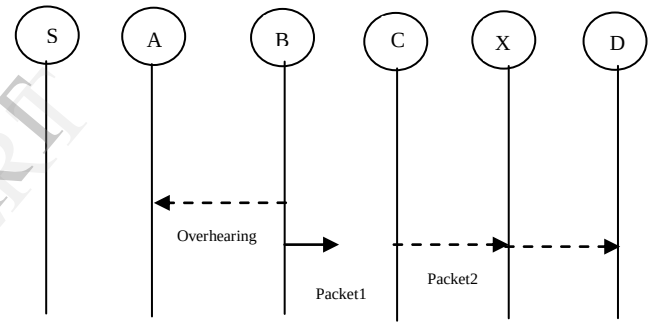

Figure 1 Limited Power Transmission

False misbehavior in MANETs,which means malicious node send a false misbehavior report about honest node. Figure 2 shows, node A and B forwarded Packet 1 to node C successfully, node A will still inform node B as misbehaving node and a false report will be send to the source.

Packet sending from the source does not reach the destination due to various reasons ie.limited power,this condition is called packet drop.

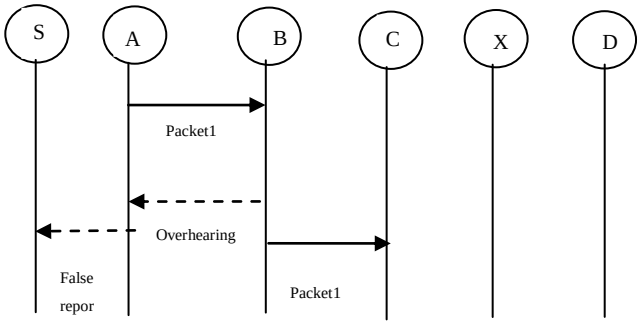

Figure 2 False Misbehaviour

This paper deals with an intrusion detection scheme ie. an acknowledgement based intrusion detection,where the detection is done according to the acknowledgement packet received at the source node which is sent by the destination node after receiving the data packet successfully.This intrusion detection also prevents the forging of the acknowledgement packets by digital signature[8] .In order to increase the security a session key has been generated and hence the forging of the acknowledgement packet can be avoided to an extent.

II RELATED WORKS

Watchdog[7] is a detection scheme which is detecting the misbehaviours of the malicious nodes in the networt ie it listens to the next hop transmission,if there is a failure in sending the packets by the next node within a certain time limit,a counter value is increased.When the counter value exeeds the threshold value, a misbehavior is detected.Pathrater then further avoids the reported misbehaving nodes in future.It main disadvantage is that the detection is not possible during receiver collision ,limited power transmission,collusion and partial packet dropping.

TWOACK is an IDS[3] which mainly deals with receiver collision and limited power transmission.Receiver collision is a situation in which two source starts transmitting packets to the same destination and there occurs a dropping of the packets.In case of limited power transmission,there is no enough power for the source to send a packet to the destination.This scheme sends an acknowledgemet packets after every two hops hence named as TWOACK.Figure 3 is showing a TWOACK scheme in which node A forwards the packet 1 to the next node ie B and then to C.Now C will send an acknowledgement packet to A with a certain limit.If acknowledgement is not reached at the node A, misbehavior nodes are detected ie, B and C. Even though it solves the problem of receiver collision and limited power transmission ,it increases the network overhead.

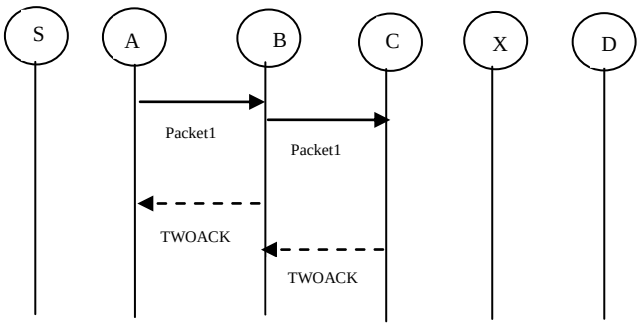

Figure 3 TWOACK Scheme

AACK[1]is an end to end acknowledgement scheme,where the acknowledgment packet is sent from the destination to the source node upon receiving the packet at the destination. This scheme is dealing with the reduction of the network overhead due to the end to end scheme as the acknowledgement packet is only sent by the destination compared to previous scheme ie.TWOACK where the acknowledgement packets are sent after every two hops.

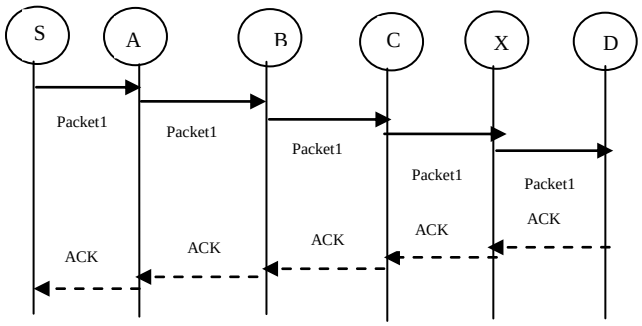

Figure 4 AACK Scheme

Figure 4 is showing an ACK scheme in which a packet is sent from source S and the intermediate nodes forwards the packets ,after the destination node receives the packet it send back an acknowledgement packet within a certain time period.

EAACK is a scheme[2] dealing with the false misbehavior report send by the malicious nodes to the source.It is an acknowledgement based scheme in which an acknowledgement packet is authenticated by encrypting the packet using the key generated by the RSA algorithm.It consists of the distribution of predetermined keys which leads the attacker to acquire the key generated and forge the message.

III SCHEME DESCRIPTION

This section mainly describes an acknowledgement based detection scheme where the acknowledgement packets confirm the delivery of the packets.Here the acknowledgement packets are authenticated using digital signature.This scheme mainly deals with the problem of distribution of predetermined key which can be acquired by attacker so that the acknowledgement packet can be forged.Random key generation is the solution which this paper is describing.Combined algorithm ie RSA[6][8] and Diffie Hellman is used to generate a random key for a particular session. Diffie Hellman is a method for generating a random key called session key for securely exchanging a shared secret between two parties, over an untrusted network. A shared secret is important between two parties who may not have ever communicated previously, so that they can encrypt their communications. Predetermined key generated in the existing system leads to more malicious attacks as the key will be easily available to the intruders so that the acknowledgement packets sent may be forged. So to overcome such a disadvantage a combination of both RSA and DIFFIE is proposed which increase the accuracy, integrity, efficiency etc.Hence the diffie key is used to digitally sign the acknowledgement packets which will prevent forging of the packet to an extent. The detection scheme consist of three modes ie ACK,SACK and MRA

The figure 6 is showing the flowchart for the scheme.This scheme consist of three parts a)ACK b)Secure ACKnowledgement(SACK) c)Misbehaviour Report Authentication(MRA)

ACK is an end to end acknowledgement mode. Initially data packet is send from source to destination through intermediate nodes.If the destination node receive the packet successfully ,it send back an acknowledgement packet to the source.If the acknowledgement mode is a failure,then it switches to the S-ACK mode.Figure 5 is showing the ACK mode in which a packet is sent from source S and the intermediate nodes forwards the packets ,after the destination node receives the packet it send back an acknowledgement packet within a certain time period else switch to SACK mode and sent an SACK packet to next mode for misbehavior detection.

S-ACK is a mode for detecting misbehaviour node.Three consecutive node work in a group to detect the misbehaving nodes.In figure 5 consider three nodes i.e. A, B and C,if A send a SACK data packet to node B and then to C.A should receive the acknowledgement packets at a predefined time, else, B and C are considered as malicious.Here A generate a misbehaviour report which is sent to source.When source is receiving a misbehaviour report then an MRA packet is generated and switches to the next mode ie.MRA

MRA scheme verify the misbehaviour report. Due to the misbehaviour report,an innocent node may be considered as malicious.

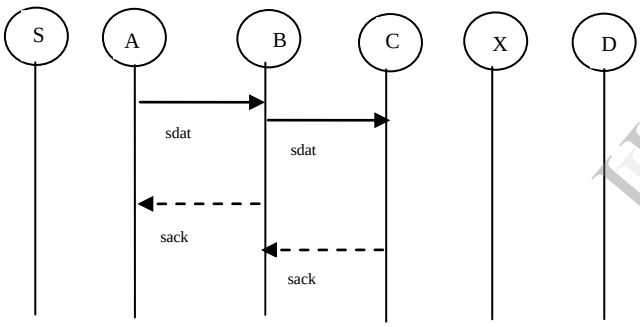

Figure 5 SACK

Initially an alternate path is selected to reach the destination node.The destination node is checked for the packet of which the misbehaviour report occurred.If the node is not having the packet then report is considered false,when the destination is having the packet then the report is marked as malicious.
Digital signature is a technique in which the acknowledgement packets to be sent is digitally signed. Here it is using MD5 for hashing the packet .A fixed length message digest is computed through a preagreed hash function for every message. Digitally signed acknowledgement packets using a diffie key will prevent the forging of the packets there by increasing the security.Session key generated using following algorithm:

Public number generated at the source X= $g^{A} \bmod r$

Public number generated at destination Y= $g^{B} \bmod r$

A and B are encrypted and decrypted key generated using RSA

r and g is automatic generated prime constants Session key generation is as follows:

$$K = KB = KA$$

where KB and KA the keys generated by the parties A and B

a. Session key generated at the source using public number generated at the destination

$$KA = Y^{A} \bmod r$$

b. Session key generated at the destination using public number generated at source

$$KB = X^{B} \bmod r$$

For encryption or decryption,XORing the packet with the session key

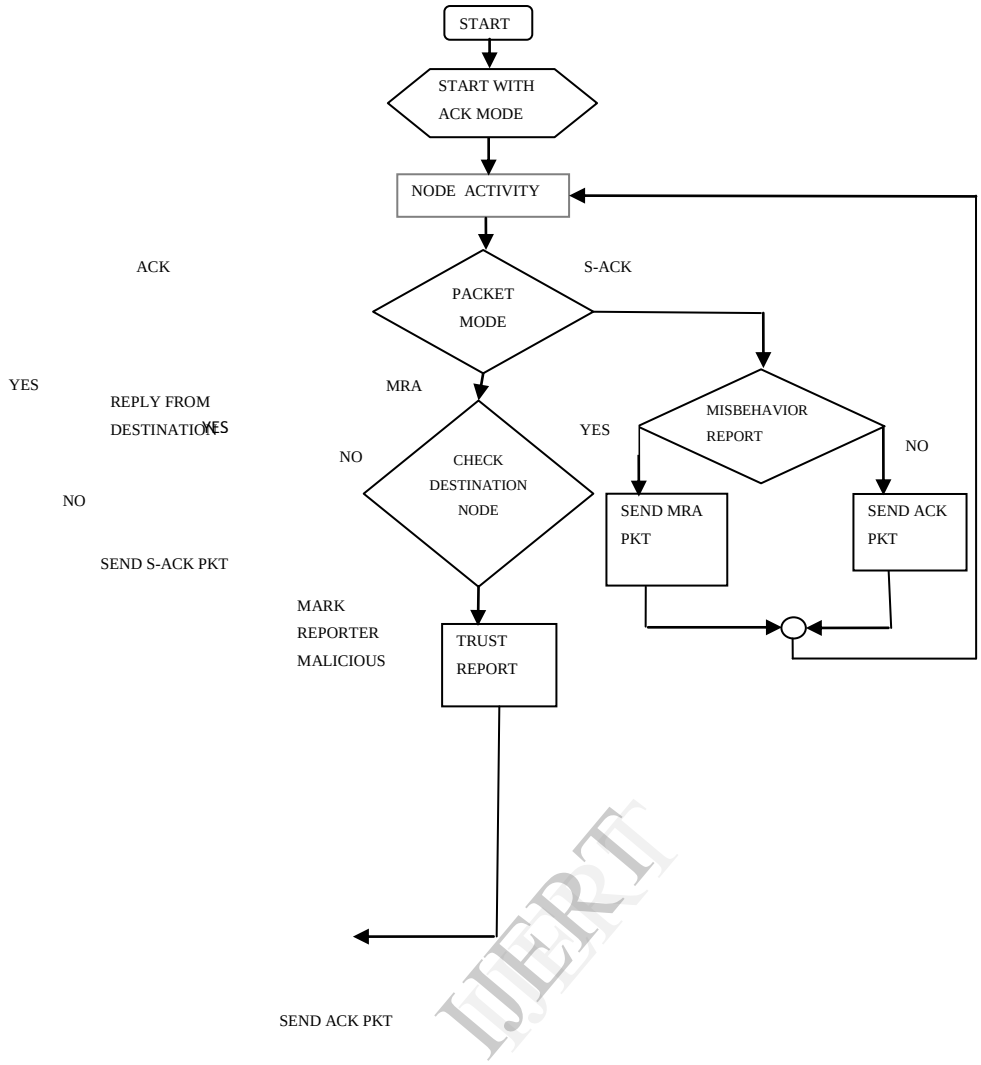

Figure 6 Flowchart

IV PERFORMANCE ANALYSIS

1.METRICS USED

The performance of this system is evaluated by comparing the Packet Delivery ratio(PDR) and Routing Overhead(RO) of the proposed system with an IDS scheme ie.EAACK.

PDR: It is defined as the ratio of total packet received by the destination node to the total packet sent by the source node

$$PDR = \frac{\text{TOTAL PACKET RECEIVED}}{\text{TOTAL PACKET SENT}}$$

RO:It is the ratio of total routing packets transmitted to the total packets send.

$$PDR = \frac{\text{ROUTING PACKETS}}{\text{TOTAL PACKETS SENT}}$$

2. SIMULATION RESULTS

Simulation is done using Network Simulator (NS 2.35).The simulation environment consist of 30 mobile nodes .Each communication of nodes is in 20 s and protocol used is AODV.The packet delivery ratio and routing overhead is obtained at different speed.

Packets will be dropped when there is a malicious node in the path determined.During simulation,for every communication a random key is generated which encrypts or decrypts the packets transmitted.

a)PDR: Figure 7 shows a graph of packet delivery ratio vs speed of the node, there is an increase in the packet delivery ratio of the proposed system than the existing system.

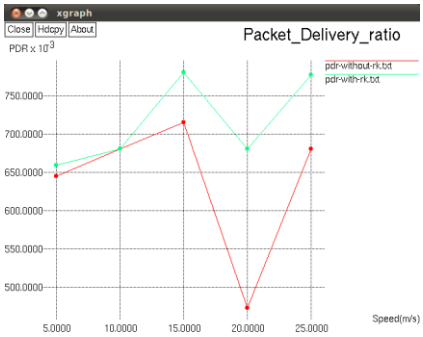

Figure 7 Packet Delivery Ratio

b)RO: Figure 8 shows a graph of routing overhead vs speed of the node.Due to the the usage of the cryptographic technique ie RSA and diffie hellman ,the overhead has been increased for the proposed system than the existing system.

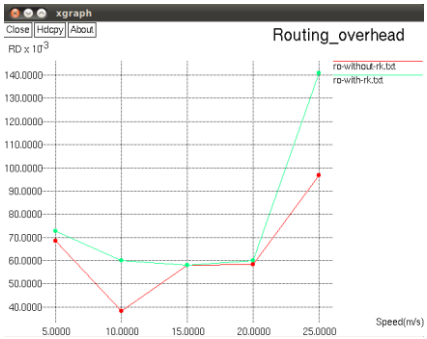

Figure 8 Routing Overhead

V CONCLUSION AND FUTUREWORK

An enhanced adaptive acknowledgement IDS using random key generation is an intrusion detection scheme for MANET's.Compared to the previous system ,the proposed system has higher security.Random key generation using diffie hellman key exchange algorithm which is exchanged between two parties. A shared secret is important between two communicating parties, so that they can encrypt their communications. Simulation shows an increase in overhead in the proposed system due to the usage of cryptographic technique for encrypting and decrypting the packet in the communication. In comparison proposed system has higher packet delivery ratio than the existing intrusion detection system hence the security is increased.

In future a hybrid cryptographic technique can be used to reduce the overhead generated due to the usage of cryptographic techniques.

REFERENCES

[1] A Al-Roubaiey†, T. Sheltami, A. Mahmoud, E. Shakshuki, H.Moufta King Fahd "AACK:Adaptive Acknowledgment intrusiondetection for MANET with node detection enhancement" ,IEEEInternational Conference on Advanced Informtion Networking and Applications,2010.

[2] EAACK – A Secure Intrusion Detection System for MANETs Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang and Tarek R. Sheltami, Member, IEEE

[3] Kejun Liu, Jing Deng, Member, IEEE, Pramod K.Varshney, Fellow,IEEE, and Kashyap Balakrishnan, Member, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior inMANETs ",IEEE TRANSACTIONS ON MOBILE COMPUTING,2007.

[4] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[5] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535–541.

[6] R. Rivest, A. Shamir and L. Adleman. A Method for Obtaining Digital Signatures and Public-key Cryptosystems.Communications of ACM 21 (2): 120-126, 1978.

[7] Y. Xiao, X. Shen, and D.-Z. Du (Eds.), "A Survey on Intrusion Detection in Mobile Ad-hoc Networks," Wireless/Mobile Network Security, pp. 170-196, 2006

[8] W.Stallings, "Cryptography and Network Security 4th Ed,"Prentice Hall , 2005,PP. 58-309.