IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 9, Issue 3, Ver. III (May - Jun. 2014), PP 100-106
www.iosrjournals.org

An Energy Efficient Acknowledgement Based Ids For Manet

Prajeena Anilkumar, Dr.S.Malathy,M.E,Ph.d
RVS college of Engineering and Technology,Coimbatore

Abstract: *Mobile adhoc network is an infrastructureless network with a dynamic native where the nodes are free to move and hence it is susceptible to various attacks. Previous system is an acknowledgement based intrusion detection system where there is a high energy condumption due to the inefficient path selection where the selected nodes energy is drained before completing the communication and also due to the flooding of hello packets to unavailable nodes. The previous IDS also has the disadvantage of pre distribution of keys which can be easily accessed by the malicious attacker which can forge the acknowledgement packets which is confirming the packet delivery. The acknowledgement packet is when forged, the false information will be delivered to the source about the honest nodes which has already successfully forwarded the packet. This project deals with the problem of high energy consumption and also attack caused by pre distribution of the keys. The acknowledgement packets are digitally signed using a session key in order to avoid the forging of the acknowledgement packets. The energy consumption is reduced by using an energy efficient path selection method where efficient nodes are selected and also by suppressing the hello packets which is sent to the unavailable nodes. Simulation tool used in this project is ns2.35 .Simulation result shows that the proposed scheme provide a reasonably good level of security and reduced energy consumption than the existing system.This system is used in the military applications,banking etc.*

Keywords: *Energydistancefactor,Diffiehellman,Digital signature,Hello message interval*

I. Introduction

MANET (Mobile Adhoc NETwork)is a flexible infrastructureless network having many mobile nodes which are moving randomly.Nodes can be iPods,PCs,smart phones and smart sensors etc.It consist of variable routing paths for the communication between a source and destination.Due to the dynamic nature of the network it is susceptible to various attacks .MANET can be classified into: InVANETs (Intelligent Vehicular Ad hoc NETworks) deals with situations like vehicle collition,VANET(Vehicular Ad hoc NETworks) provide effective communication with other vehicles and Internet Based Mobile Ad hoc Networks (iMANET) which helps to link fixed as well as mobile nodes. Due to its wireless medium and its dynamic nature ,the network faces many problems like unpredictable topology,congestion and limited resources such as bandwidth and energy.Nodes in the MANET has different energy levels and according to the energy of the nodes,in moves randomly towards its destination.Eenergy of some nodes will be drained earlier before the communication ends.In such cases nodes selected for the communication should energy efficient.There are three security goals for MANET through which a successful communication of a source and the destination is possible ie confidentiality,integrity and authentication.Due to compromising of the security goals leads to attacks where confidentiality implies the communication without involving a third person,integrity implies the communication without forging of the packets and authentication means communication between authentic nodes.Attacks in the MANET are classified as passive attack and active attack.In case of passive attack the attacker will snoop the the data exchange without altering it there by targeting its confidentiality.The data exchanged in the network is modified by the attacker ie by dropping packets or injecting packets In such cases there is a need of an intrusion detection scheme which is a reactive mechanism.This paper is dealing with packet dropping,receiver collsion,limited transmission power and false misbehavior by the attacker nodes.Packet dropping may be due to limited power of the nodes to transmit the data to its destination.Receiver collision means a single receiver simultaneously receives data packets from two different transmitters.False misbehavior by a node implies that it sends a false misbehavior report about the honest nodes,even though the packet for which the misbahaviour report has sent is already received at the destination.Figure 1 is showing the fasle misbehavior where A and B are forwarding packets to C,eventhough c has received the packet A may send a false report to the source S by a node A.

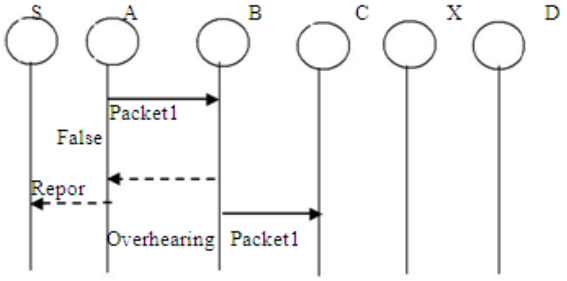

Figure 1 false misbehavior

As the intrusion detection scheme is based on the acknowledgement packets sent by the destination to the source for confirming the packet delivery to its destination.The acknowledgement packets can be forged by the attacker hence the security can be increased by generating a session key ,hence the acknowledgement packets are digitally signed before transmitting.The digitally sighned acknowledgement packets cannot be forged by the attacker there by increasing the security.This paper is dealing with another aspect ie the energy of the system.The efficiency of the system is an important aspect and it can be increased by two methods ie. by choosing an energy efficient path for a source destination pair and also by suppressing hello packets.The path selection is based on the energy level of each node hence selecting the most energy efficient nodes in its transmission range.The energy efficient intrusion detection scheme is discussed in the following sections which looks into both the security and the efficiency aspects of the detection system.

II. Related Works

Watchdog[] is a detection scheme which monitors the next hop transmission to detect the misbehaving nodes by setting a threshold value,if the packet is not receiving at the destination within this threshold value ,the misbehavior is detected.This does deals with the receiver collision,false misbehavior and limited transmission power.

TWO ACK [] is an intrusion detection system which which deals with receiver collision and limited transmission power.It is having an increased overhead.It sends an acknowledgement packets at every two hops hence named two acknowledgement scheme.

AACK[1]is an end to end acknowledgement scheme,where the acknowledgment packet is sent from the destination to the source node when packet is received at the destination. This scheme reduces 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 2 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.

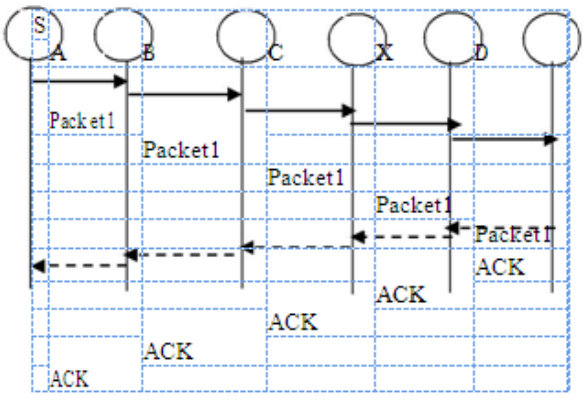

Figure 2 AACK Scheme

Previous intrusion detection systems are not considering the energy efficiency of the system .

III. Scheme Description

This is an energy efficient acknowledgement based intrusion detection scheme.This paper is dealing with both security and efficiency aspect.Detection consists of three modes ie.ACK,S-ACK and MRA(Misbehaviour Report Authentication as shown in the flowchart in figure 3.The delivery of the packet to its destination is confirmed by the acknowledgement packets.

The three modes are:

ACK is an end to end acknowledgement scheme where a source send a packet to the destination,it send back an acknowledgement packet to the source confirming the delivery of packet.If the acknowledgement packet does not reach the source at a particular predetermined time then it switches to S-ACK mode and send an S-ack packet.

SACK is a mode where the misbehaving nodes are detected.In figure. 2 it considers three consecutive nodes 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

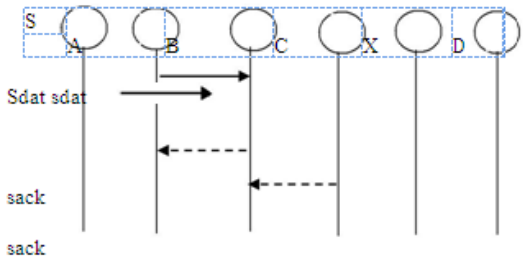

Figure2 SACK Scheme

After the misbehavior report is sent to the source,MRA scheme begins in which an alternative path is selected through which the misbehavior report is sent to the destination.Destination node now checks for the packet for which the misbehavior report is sent.If the destination node contains the packet ,then the misbehavior report is false and the node which sent the misbehavior report is malicious.

When the security aspect is considered,the acknowledgement packet sent for the detection is digitally signed using a session key generation for each source destination pair.The session key is generated by combination of RSA and Diffie Hellman .Hence the security is increased as the key cannot be easily acquired by the attacker and the acknowledgement cannot be easily forged.Key is generated using the following algorithm in which a session key is generated wich will digitally sign the acknowledgement packets.

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

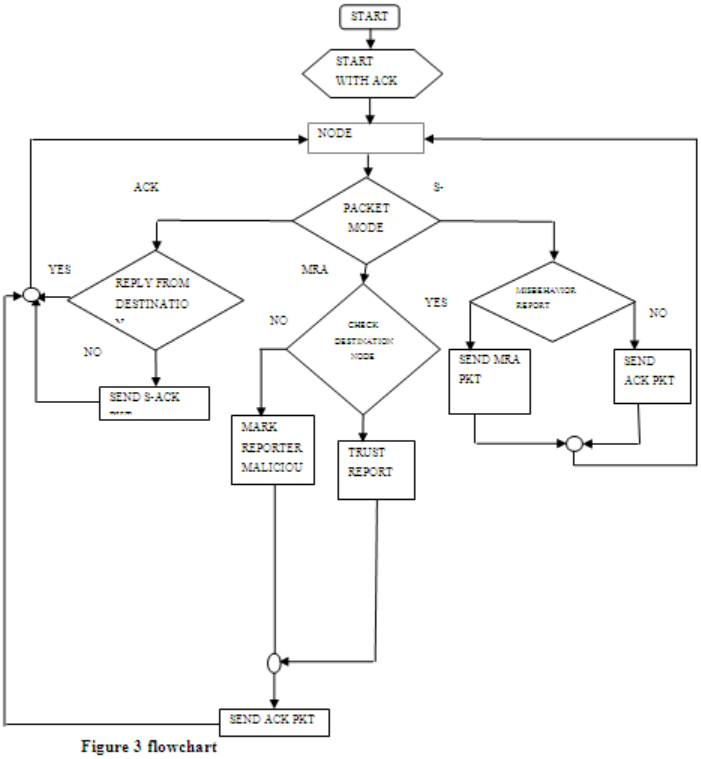

Figure 3 flowchart

Energy aspect of the IDS when considered,its efficiency can be increased by two methods ie. Selection of the path based on energy distance factor and by suppressing the unnecessary hello packets. a PATH SELECTION BASED ON ENERGY DISTANCE FACTOR

Each node in the MANET have different energy levels,hence the most efficient node is selected for each hop.The network is categorized as tiers based on the hop distance nodes in tier2 and so on as shown in figure 4

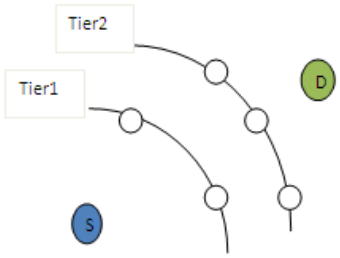

Figure 4 energy zones

Energy distance factor (ρ) is calculated as:

$$\rho = \frac{e_x d_x}{\sum e_x d_x}$$

e is the energy and d is the distance of node from source

The highest energy distance factor node is selected in each tier ,hence an intermediate node is selected for the particular source destination pair.

b. SUPRESSING HELLO PACKETS

Another energy saving method is to suppress unnecessary hello messages which may drain the batteries even when yhe mobile is not in useie.suppress the hello packets sent for the unavailable nodes.This is possible by dynamically changing the hello interval based on event interval ,hence if the event interval is large then the hallo interval will be large.Large hello interval implies, suppressing of most of the hello packets of the unavailable nodes.Event interval is the time gap between two consecutive events.

X = (ALLOWED_HELLO_LOSS-0.5)*HELLO INTERVAL

x= event interval

IV. Performance Analysis

Simulation is done using Network Simulator (NS2.35).The simulation environment consist of 100 nodes .For different number of nodes ,the packet delivery ratio,energy consumption,overhead,,delay has been obtained .Malicious node is detected when the acknowledgement packet does not reach the destination.

Table 4.1 Average energy consumption

SL NO	No. of nodes	EAACK	EEAACK	HNEAACK
1	50	0.087824	0.467438	0.121325
2	60	0.102099	0.815581	0.07994
3	70	0.101269	0.8567	0.02966
4	80	0.142035	1.13295	0.117508
5	90	0.167429	1.26261	0.04525
6	100	0.166266	1.39058	0.087370

Average energy consumption total consumed energy of all nodes after data transmission HNEAACK energy is reduced considerably due to the energy efficient path selecton ans suppressing of hello packets.Table 4.1 shows different values of energy consumption for different number of nodes. Figure 5 is an energy consumption vs number of nodes showing a reduced energy consumption than EAACK and EEAACK.

Throughput is defined as the total number of packets delivered over the total simulation time. Table 4.2. is showing different throughput values for different number of nodes,there is an increase in the thoughput for HNEAACK when compared to both EAACK and EEAACK. Figure 6 is showing the throughput vs number of nodes,where the throughput is analysed for different number of nodes.HNEAACK is showing greater throughput compared to EAACK and EEAACK.

Table 4.2 Throughput

SL NO	No. of nodes	EAACK	EEAACK	HNEAACK
1	50	80160	79520	80160
2	60	80161	65760	80162
3	70	80162	68480	80161
4	80	80160	41920	79840
5	90	80164	24320	73440
6	100	80159	20640	78880

Normalised Routing Overhead is defined as the data bits added to user transmitted data for carrying routing information, error correcting and operational instructions

Table 4.3 Normalised Overhead

SL NO	No. of nodes	EAACK	EEAACK	HNEAACK
1	50	0.009634	0.123475	0.0999465
2	60	0.0999362	0.123476	0.099938
3	70	0.0999372	0.1183	0.0999377
4	80	0.0911069	0.194549	0.0958205
5	90	0.0995169	0.31503	0.0999119
6	100	0.0947088	0.32329	0.0999031

Table 4.3 shows a normalized overhead for different number of nodes,where the normalized overhead is reduced in the HNEAACK than EAACK and EEAACK as the hello packets will be suppressed for unavailable nodes. Figure 7 is showing the normalized overhead vs number of nodes,where the packet normalized overhead is analysed for different number of nodes.HNEAACK is showing lowest overhead compared to EAACK and EEAACK,due to the hello suppressing method used in HNEAACK.

Jitter is defined as the time gap between packets or it can be defined as the variation in the time between packets arriving, caused by network congestion, timing drift, or route changes Table 4.4 is showing different jitter values for different number of nodes,it can be observed that there is large jitter values for EAACK and low values of jitter for EEAACK and HNEAACK. Figure 8 is showing the graph for jitter against number of nodes, where the jitter is analysed for different number of nodes.HNEAACK is showing lowest jitter except for some number of nodes in EAACK.

Table 4.4 Jitter

SL NO	No. of nodes	EAACK	EEAACK	HNEAACK
1	50	0.009634	0.123475	0.0999465
2	60	0.0999362	0.123476	0.099938
3	70	0.0999372	0.1183	0.0999377
4	80	0.0911069	0.194549	0.0958205
5	90	0.0995169	0.31503	0.0999119
6	100	0.0947088	0.32329	0.0999031

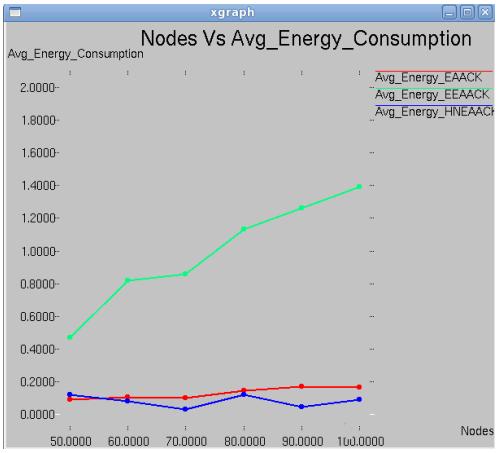

Figure 5 Average Energy Consumption Vs No of nodes

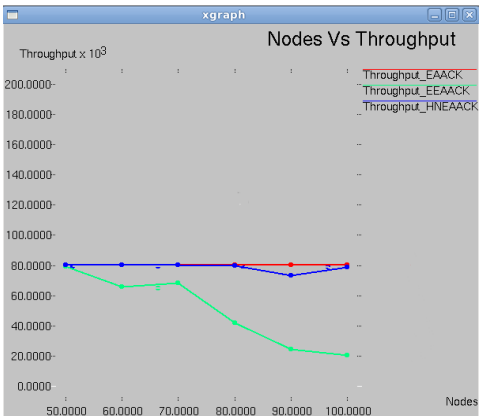

Figure 6. Throughput Vs No. of Nodes

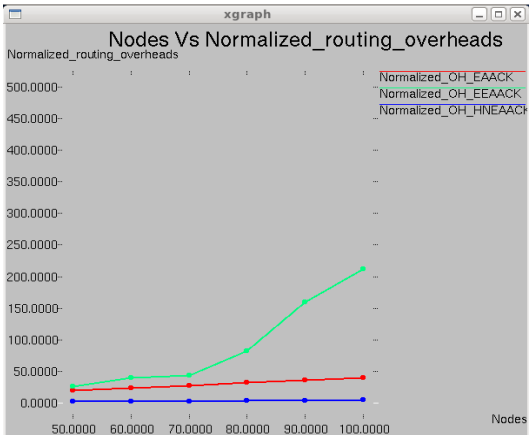

Figure 7 Normalised Overhead Vs No. of Nodes

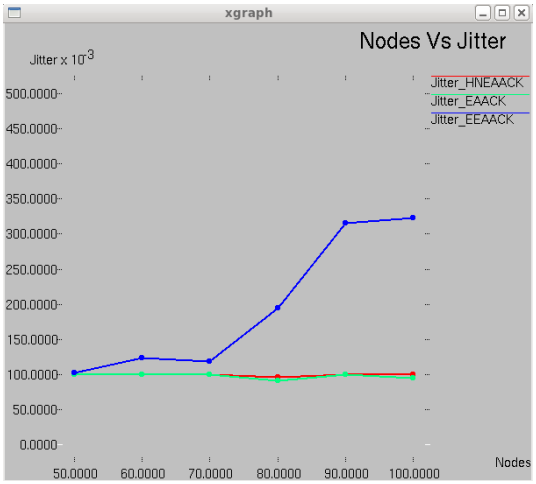

Figure 6.6 Jitter Vs No. of Nodes

V. Conclusion And Futureworks

An efficient acknowledgement based IDS for MANET is an acknowledgement based detection system .Compared to EAACK the proposed system has higher security and increased energy efficiency.The generation of the session key for particular source destination pair will increase the security,as the session key digitally sign the acknowledgement packet preventing forgery.Diffie hellman is the effective key generation method used. When efficiency is considered,the use of two energy efficient methods such as efficient path selection and suppressing of the hello packets for the unavailable nodes will reduce the energy consumption considerably than previous system.Efficient path selection includes the high energy intermediate nodes ,which is selected using energy distance factor.HNEAACK is providing a higher packet delivery ratio,throughput and a reduced energy consumption ,delay,overhead and jitter when compared to EAACK and EEAACK

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

References

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

[2]. Eleni Darra,Christoforos Ntantogian,Christos Xenakis,Sokratis Katsikas(May 2010) "Prolonging the Lifetime of wireless sensor networks via hotspot analysis" in International Colloquium on Computing, Communication,Control and Management (CCCM2009),Vol 6, pp. 421-428

[3]. Elhadi M. Shakshuki, NanKang, andTarekR.Sheltami(March 2011), "EAACK— A Secure Intrusion-Detection System for MANETs" IEEE journal on industrial electronics, Vol. 60, pp 1089-1098

[4]. Giruka.V.C and Singha.M(January 2005)l, "Hello protocols for ad-hoc networks: overhead and accuracy tradeoffs," Proceedings of Sixth IEEE InternationaL Symposium on a World of Wireless Mobile and Multimedia Networks,pp. 354–361

[5]. Hoang Lan Nguyen,Uyen Trang Nguyen(July 2006) "A Study of different types of attacks on multicast in mobile adhoc networks"Proceedings of IEEE WMCSA'06,Vol 9,pp 32-46

[6]. Kejun Liu,Jing Deng,Pramod K.Varshney(2007) "An Acknowledgement-Based Approach for the Detection of Routing Misbehaviour in MANET's,IEEE journal on Mobile Computing,Vol .6,pp 117-125

[7]. Ms.Sonali P .Botkar,Mrs.Shubhangi R Chaudhary,(May 2007) "An enhanced intrusion detection system using adaptive acknowledgement based "World Conference on Information and Communication Technologies,Vol 3,pp 606-611

[8]. Roubaiey.AL,T.Sheltami,A.Mahmoudi(March2010)"AACK:Adaptive acknowlwdgement intrusion detection for MANET with node enhancement", 24th IEEE Inrenational Conference

[9]. Vaithiyanathan S,Edna Elizabeth N(September 2010) "A Novel method for Self management of the energy consumption of nodes dying out of low battery capacity in a NTP based routing environment of MANETs" Proceedings of International Conference on Information Technology,Next Generations, pp. 101–108

[10]. Vahid Heydari(April 2012)"A New Acknowledgement-based Scheme Against Malicious Noded and Collusion Attack in MANETs" in Proceedings ACM International Conference on Mobile Computing,Vol 3.pp 1123-1128

[11]. Wang J., de Dieu I.J., Jose A.D.L.D., Lee S., and Lee Y.K(April 2010) "Prolonging the Lifetime of wireless sensor networks via hotspot analysis," in International Symposium on Applications and the Internet (SAINT), pp. 383-386

[12]. Rajeshkumar.G,K.R.Valluvan(APRIL 2013), "A Comparative Study of Secure Intrusion Detection Systems For Discovering Malicious Nodes on MANETs",International Journal on Computer Applications,Vol 18,pp 1-5