Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 8, August 2015, pg.86 – 90

RESEARCH ARTICLE

An Acknowledgement Based Malicious Node Detection For MANETS

I.Maria Sabatni[1], E.Ramaraj[2]

M.Phil Scholar[1], Professor[2]

Department of Computer Science and Engineering, Alagappa University, Karaikudi, India

Email: mariasabatni3@gmail.com

Abstract: Mobiles are widely and commonly used thing in the world. Because of it's mobility and scalability. Mobility is achieved through the Manet which was wireless network. So it has no fixed infrastructure and it don't need physical wired connections.It is widely. MANET is short form of Mobile Adhoc Network.MANET is a collection of many individual mobile nodes.MANET met many problems like low transmission power,receiver collision,occurance of malicious node. The proposed scheme Secure EAACK remove the problem of malicious node ocurrance. This paper concentrate the malicious detection and removal.

Keywords: Digital signature, digital signature algorithm (DSA),Secure Acknowledgement,(S-Ack), Enhanced Adaptive Acknowledgment (AACK) (EAACK), Mobile Ad hoc Network (MANET).

1. Introduction

Shaksshuki et al(2013) have discussed that the security problem in MANET because of it's lack of fixed infrastructure. In their work it has been focused a new intrusion-detection system named Enhanced Adaptive Acknowledgement(EAACK) specially designed for MANET. Sari et al(2014) have discussed that the security issues in MANET for researchers based on [DOS] Denial of Service attacks. In their work it has been focused USM(Unified Security Mechanism and Rate Adaptation Scheme (RAS) methods are used against DOS attack. Shivashankar et al(2013)have discussed that the problem of power consumption . In their work it has been focused the usage of new routing protocol(EPAR) Efficient Power Aware Routing , that increases the networks lifetime of MANET. Forne et al (2009) have discussed that the certificate validation problem in MANET'S Authorities are not guaranteed. In their work

it has been focused the suitable certification validation process for MANET by cooperative mechanism used nowadays. Ghabretensae et al (2010) have discussed that increasing the capacity of backhaul network and increase network utilization and decrease operating expenses. In their work it has been discusses different migration scenarios from the circuit – switched legacy backhaul networks toward Packet-based networks. Gonzalvez et al have discussed that channel allocation mechanisms evaluated. In their work, improve the QOS compared to the traditional random allocation mechanism while also offering it's benefits in terms of uniform long term channel use. Hur et al(2014) have been discussed that the quality and functionality of the filters is to ensure a decoupling of unknown acceleration. In their work it has been discussed that the developed filters to minimize the external disturbance effects. Ju et al (2007) have been discussed that the mobile backbone network topology synthesis algorithm for constructing and maintaining a dynamic backbone structure for MANET. In their work it has been presented an on-demand routing Protocol(MBNR) that makes use of the underlying dynamically self configuaring backbone network infrastructure and demonstrate it's performance. Song et al(2013) have been focused excessive energy consumption in mobile sensor networks. In their work it has been introduced two algorithms named Lloyd which saves travelling distance and DEED(Distributed Energy –Efficient self-Deployment which is less energy consumption.

2. Existing Work

Many existing approaches for MANET to overcome the network security problems. In this case ,mainly three approaches are used for intrusion detection in MANET.

They are

1.watchdog
2.Twoack
3.Adaptive Ackowledgement
4.Enhanced AACK

1.Watchdog

Watchdog is used in MANET improve the troughput of network with the presence of malicious nodes. It has two parts.

a.watchdog
b.pathrater

a)watchdog

The first part is responsible for detecting malicious node misbehaviors. If a watchdog fails to forward the packet within a certain period of time,it increases it's failure counter.

b)pathrater

Pathrater cooperates with the routing protocols
To avoid the reported nodes in future transmission.

Advantage:

Capable of detecting malicious nodes.

Limitations:

It fails to detect malicious misbehaviors.

2.TwoAck

This scheme is designed for resolving the watchdog's problem. It detects every data packets transmitted every three consecutive nodes along the path from the source to the destination.

Limitations:

Acknowledgement process increase network overhead.
Repeated tramnsmission process can easily affect transmission power.

3.AACK

AACK scheme was based on Twoack which reduces the network overhead which is occurred in watchdog

Limitations:

Fail to detect malicious nodes with the presence of false misbehavior report.

4.Enhanced AACK

In EEACK scheme specially used digital signature for secured tranmission.Every transaction digitally signed by it's sender and verified by it's receiver. So it resolves receiver collision,limited transmission power,false misbehavior report.

Limitations:

Time delay for choosing right path for transactions because of searching unintruder path.

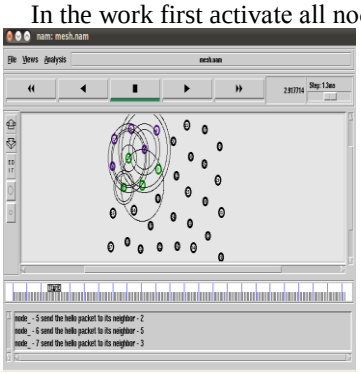
3. PROPOSED WORK

The proposed work is based on the EEACK scheme and reduce the limitations in the EAACK scheme.In the work it exactly detect the malicious node.

Working Process:

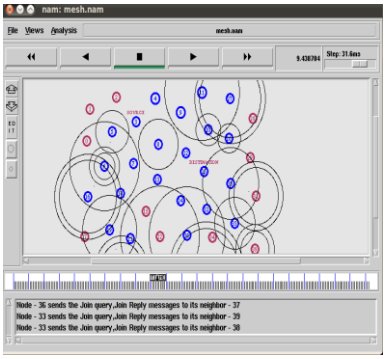
Step 1:

In the work first activate all nodes in the base station by sending hello messages to it's neighbor node.



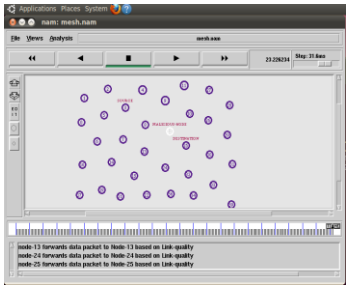
Step 2:

Detect source and destination node by sending join query and join query reply messages to it's neighbor.



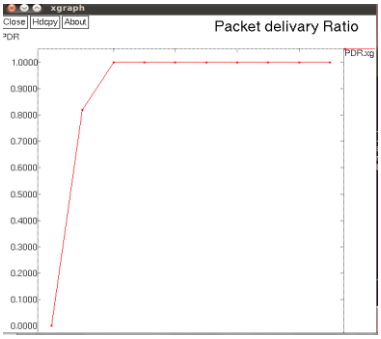
Step 3:

Drop the malicious node which is detected in the second step.

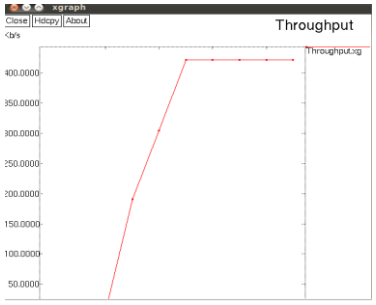


Advantages:

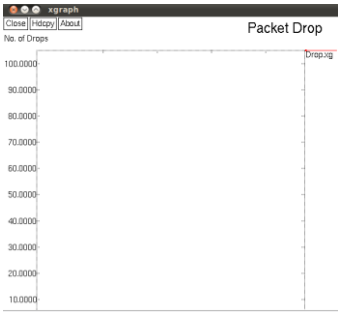
Packet delivery ratio is increased which is compared to the previous schemes.



Throughput was also increased compared to the previous methods.



Packet dropping ratio is also increased because detect the accurate malicious node.



4. Conclusion

Malicious attack is a major security problem in MANETs. In this research paper, we have proposed a secure malicious detection specially designed for MANETs. It provides less time to deliver packet because in our work first know the activated nodes.

It also inform it's neighbor which is a malicious node.It ensures secure transfer of data among mobile nodes.

References

[1] Shaksshuki , EM , Kang , Nand Sheltani , TR , 2013 , 'EAACK – A Secure Intrusion-Detection System for MANETS' , IEEE Transactions on industrial electronics , vol.60 , No 3 PP 1089 – 1098..

[2] Sari , A , 2014 , 'Security approaches in IEEE 802.11 MANET ' IEEE Network and System science 7 , PP 365 – 372-292.

[3] Shivashankar , Suresh H.N , Varaprasad Golla , 2013 , 'Designing Energy Routing Protocol with power consumption Optimization in MANET ' , IEEE Transactions on Emerging topics in computing , 10.1109/ TETC.2013.2287177.

[4] Hur , H and Ahn , H.S ,2014 , 'Unknown Input Observer – Based Filterings for mobile pedestrian Localization using wireless sensor networks ' , IEEE sensors journal , vol 14 , no-8 , PP 2590 – 2600 .

[5] Song , Y , Wang , B , Shi , Z ,Pattipati and Gupta , S(2013) , 'Distributed Algorithms for energy-efficient even self-deployment in Mobile Sensor Networks' , IEEE Tranctions on Mobile computing , PP 1-14.

[6] Tunca ,C , Isik , S .M , Donmez , Y and Ersoy , C(2014) , 'Distributed Mobile Sink Routing for Wireless Sensor Networks: A Survey ' , IEEE Communications surveys and tutorials , vol .16 ,no.2 ,PP 877 – 897.

[7] Zhang , J , Zhang , Q , Li , B , Luo , X , Zhu , W(2006), Energy-efficient Routing in Mobile Ad Hoc Networks: Mobility – Assisted Case' ,IEEE Transactions on vehicular Technology , vol .55 , No.1,PP 369 – 379.

[8] Lin , Y . B , Lee , P . C , Chlamtac , I(2002) , 'Dynamic Periodic Location Area Update in Mobile Networks' ,IEEE transactions on vehicular Technology , vol .51, No .6, PP 1494 – 1501

[9] Wu , H , Wang , Y , Dang , H and Lin ,F(2007) , "Analytic , Simulation, and Empirical Evaluation of Delay/ Fault-Tolerant Mobile Sensor Networks' , IEEE Transactions on wireless communications , vol.6 ,no.9 , PP 3287 – 3296.

[10] Vazquez , A.J.L , Felipe , A , Perez , C and Guerrero , L.O (2006) , 'Performance Analysis of Fractional Guard channel policies in mobile cellular Networks ' ,IEEE Transactions on wireless communications , vol.5 , no .2 , PP 301 – 305.

