Secured PSR based Routing Protocol for Detection of Packet Dropping Attacks using Two Acknowledgement Scheme in MANET

P. Ramesh
Dept. of Computer Technology
Anna University, MIT Campus
Chennai,
India

H. Abdul Rauf, PhD
Principal,
Dhaanish Ahmed Institute of Technology
Coimbatore, India

C. Arunbritto
Anna University, MIT Campus,
Dept. of Computer Technology
Chennai,
India

ABSTRACT

Mobile Adhoc Networks (MANETs)are mainly design for node to node communication without any base station, node without transmission range support nearest node to send the data packet. The nearest node won't send the packet to the destination node, because it act as the malicious or any valid reason. According to this situation, we need grantee to sending and dropping packet. Existing work mainly focus on the DSR based protocol, in this protocol on demand protocol and it take more time to identify the destination. In this paper use PSR protocol knowledge about the all node continuous update the routing information in routing table. The collect information using two acknowledgement based scheme in opposite of traffic route in the network. In this two acknowledgement PSR based scheme more effective compare existing acknowledgement mechaisum. This types of intrusion detection mechanism choose the alternate path in the network and more efficiency to send the data packet.

Keywords

DSR (Dynamic Source Routing), IDS (Intrusion Detection System), MANET (Mobile Adhoc Network),PSR (Proactive Source Routing), 2ACK (TWO Acknowledgement)

1. INTRODUCTION

The Mobile Adhoc Networks are infrastructure less networks that communicate within the communication range. The node not within the transmission range supporting intermediate node to sending data or information, during this time intruder retrieve this information and modified that data and information, this is known as attack [1]. The attack classified two type active attack and passive attack. In active attack is modified, damage, destroy and dropping the data packet.A Mobile Adhoc Networks (MANETs) is a continuously self-configuring, self-forming infrastructure-less (without Base station) network of mobile devices joined without wires. This results in a highly dynamic, autonomous topology[2].

Mobile Adhoc Network has many independent mobile nodes, in which each of these nodes interconnect with other nodes in the range directly using radio waves. While the other nodes that are out of range need the help of middle nodes to path their packets. In this networks work by themselves or it may be associated to the bigger platform. Every nodes has a wireless interface to connect with other nodes in the network.

The basic task in construction a MANET is to equip every device such that the evidence required for traffic route is maintained continuously. The MANETs are fully disseminated, so, it can operate at everyhabitation without any static infrastructure or central coordinator as base stations or access points. Due to these characteristics, basic routing protocols cannot be used and some specific ones have been proposed. As routing activity is necessary in a MANET network formation, it constitutes a privileged target of attackers. In this Mobile ad hoc networks are separately self-organized networks deprived of the help of a central coordinator [6]. In a mobile ad hoc network nodes changing randomly, the network may unpredictable changes andknowledgequickin the topology. And since nodes in the MANET normally have partial communication ranges, they can't directly communicate with all nodes in the network. Hence, routing paths in mobile ad hoc networks usually have numerous hops and each node in mobile ad hoc networks has the responsibility to act as a router[12].

1.1 Routing Protocols

There are three kinds of routing protocols in MANET. They classified as proactive routing protocols, reactive routing protocols and hybrid routing protocols.

1.1.1 *Reactive Routing Protocol*

In reactive routing protocol, each nodes in the network maintains the route information only if there is a necessity exists for finding new route. For every route identification procedure there must be a route search to the new destination [4]. This on-demand method of routing protocol reduces the overhead of routing. Since MANET has the rapid change in the network topology, the active route may break and leads to frequent route search. AODV, DSR and CBPR are the reactive routing protocols.

1.1.2 *Proactive Routing Protocol*

In proactive routing protocol, the nodes are always maintainthe complete routing information of the network. This is possible by broadcasting messages periodically with the changes and the routing information to find the current status of the network topology. DSDV and WRP are the proactive routing protocols. A Light Weight PSR [2] protocol is high efficiencycompare DSDV, DSR routing protocol. In this PSR protocol reduce broadcast information

PSR can maintain supplementary network topology information than distance vector routing to help source routing. In this protocol, each node maintains a breadth first search spanning tree of the network rooted at its node [7]. This information is periodically send among neighboring nodes for updated network topology information. Thus, Proactive Source routing allows a node to have full-path information to all other nodes in the networks. AODV, DSDV and other DV-based routing algorithms were not designed for source routing algorithms were not designed for source routing this protocol not suitable for opportunistic data forwarding [2]. The reason every node in these protocols only knows the next hop to touch a given endpoint node but not the complete path. OLSR protocol MPR technique not sufficient [3]. Thus, we put forward a tree based routing protocol. PSR which inspired by PFA and the WRP.PSR route messaging is designed the periodic route update using hello message, converted binary tree to reduce the size of the payload by about a half and interleave full-dump message with differential updates.

1.1.3 *Hybrid Routing Protocol*

Hybrid routing protocols are the combination of reactive and the proactive routing protocols. Hybrid protocol are used to overcome the disadvantages of both proactive and reactive protocols since reactive protocols have large overhead and proactive routing protocols have large latency. Hybrid is the junction of both the other protocols. Cluster based routing protocols are the hybrid routing protocols and ensure highly stable network[5]. Advantages of CBRP are high PDR, avoid routing overhead, lesser network traffic, minimal information stored, communication scalability, route maintenance and route shortening.

1.2 Attacks in MANET

1.2.1Passive attacks

In this positive attack doesn't modified data or information presented network. But it can be "listening" what activities going on in traffic in alternative way. In this attacks are mainly focus on retrieve some information and disrupt the operation of a routing protocol. Some encryption mechanism used to overcome this situation from routed traffic.

1.2.2 Active attacks

In this active attacks are changing and destroy activities in presented network that avoid message sending through network. The active attacks are mainly two categories, it can internal and external attack. Internal attacker that present as usual activities of presented network, in this malicious activities not easily to detect than the external attack. External attacker try to communicate the presented network without permission neighbor node. The attacker to make changes such as modification of packets and retrieve the information to the communication information.

1.2.2.1 Physical Layer attacks

In this layer identified some of the attacks such as jamming, eavesdropping etc.

Eavesdropping: It can be message reading and conversations by without knowledge of communicator. The main aim retrieve confidential information and take out the information.

Interference: It is a denial of service attack which blocks the wireless communication channel, or damage communications.

1.2.2.2 Data link layer attacks

In this data link layer can classify attacks as to what effect it has on the state of the network. The selfish misbehavior nodes drop the packets intentionally in order to save battery power and energy resources.

Nodes behavior of Malicious

The malicious node main task is disrupt the normal process of routing protocol. The impact of such attack is increased when the communication takes place between neighboring nodes.

Denial of Service:
To avoid the delaying in time-critical operation using authorized prevention mechanism. The delay in legitimate network traffic in "flood" network. In this attack detect and defend difficult because it is a malignant attack.

Misdirecting traffic
A misbehavior node send wrong routing information in order to retrieve authentication data before the actual route.

1.2.2.3 Network Layer attack

Black Hole Attack
In this attack drop all sending packet through the forged route advertised. How to happen means node advertises another node that it has shortest route will be established the malicious node. The malicious node can drop packet perform man in the middle attack or DOS attack.

Impersonation Attack
The node is free to move anyway in network because it have no secure authentication process, so easily attacker will enter network and do some malicious activities. In this mobile adhoc network uniquely identifies the host in IP and MAC address. This is not enough for the authentication sender, so attacker easily get information from one node and hide into the network. Another name of in this kind of attack is called spoofing attack.

Routing table poisoning attack
In this attack change the routing table information and change the position of sending packet information. It is inject route request (RREQ) packet with biggest sequence number will be removed in table. So this leads to send wrong routes.

Rushing Attack
In this rushing attack send more number of route request to target nodes. The target node to reject valid route request node because it confusion and attacker node insert the communication without knowledge of target node.
Packet dropping attack
The packet is forwards from sender, the next intermediate node usually forwards the packet to the next node. The third node which acts as a malicious node does not forwarded the packet to next node and drops the packet. So no node after third node receive the packet.

Packet dropping attack, the attacker attacks in the network and introduce unwanted delays in the network. In this type of attack, the attacker node first get access to the network, once it get into the network and became a part of the network. The attacker then introduce the delays in the network by delaying all the packets that it receives, once delays are propagated then packets are released in the network. This enables the attacker to produce high end-to-end delay, high delay jitter and considerably affect the performance of the network.

A node that is supposed to relay packets instead discard them. Unsteadiness of the medium a may be dropped due to contention in the medium, congestion and corruption in the medium and packet may be dropped due to broken link.

A Packet dropped due to lack of energy resources, selfishness of a node to save its resources and a packet may be dropped due to malignant act of malicious node.

1.3 Acknowledgement Schemes

The MANETs consists lot of drawback according to this situation to detect and minimize the attack using secure acknowledgement based intrusion detection mechanism[18].

1.3.1 Watch Dog

In this watch dog scheme improved the throughput of network. Here each and every node sending acknowledgement packet to the sender node continuously, so watch dog scheme wrongly identified the packet dropping attack because of it collision. Overcome in this situation we need effective protocol, these protocol complete knowledge of topology information.

1.3.2 One Acknowledgement

Avoid watch dog problem like overhearing, receiver collision and limited transmission power. A single acknowledgement scheme sometime drop the packet, that time packet identified not easily. In this situation increased the hop count of network and minimize the dropping.

1.3.3 Selective Acknowledgement

Less overhead than one acknowledgement scheme. In this situation acknowledgement packet receive the destination take more time. To avoid this situation proposed random way to sending data packet and increased the RTR and CTS count value.

1.3.4 Two Acknowledgement

It is more reliable than one acknowledgement and selective acknowledgement scheme. TWO Acknowledgement based scheme send data packet to the opposite of data traffic route .According to this situation access time increased using BEB Algorithm but sometime sender node wrongly identified, because of overhearing techniques.

1.3.5 Selective Two Acknowledgement

Derivative of TWOACK scheme and less overhead than two acknowledgement method. In this techniques not identified packet sending and receiving operation and it take more time to take packet to reach the destination. Packet encryption techniques to protect the packet and send the packet to opposite direction.

1.3.6 Adaptive Acknowledgement

In this scheme detect both link and node and similar to TWOACK scheme. Adaptive acknowledgement mechanism similar to the end –to –end acknowledgement based method that access to different routing protocol using particular count value. The count value not easy to set because count value not easily to predict the previous operation.

1.3.7 Enhanced Adaptive Acknowledgement

In this scheme used for digital signature to protect the packet. It take more battery power because of high computation operation.

Random Two Acknowledgement

Extension of Two acknowledgement scheme and less overhead than two acknowledgement because of random acknowledgement.

1.3.8 N-ACK

In this Number of node acknowledgement method high reliable and very high network overhead.

Timer based acknowledgement Reduces delay, overhead, and packet drop compared to other scheme.

2. RELATED WORK

Most of the previous works on attacks have mainly focused in proactive routing protocol such as OLSR and DSDV protocol.

Djenourito and Nadjib Badache have proposed two hop acknowledgement scheme to overcome the drawback of passive-feedback scheme using power control. Here used authentication mechanism to prevent the forged acknowledgement packet. The major disadvantage of this scheme is the huge overhead of receive packet. In this situation author proposed sending the packet randomly using MPR (Multi point Relay) techniques, in this techniques reduce the huge overhead , but it take more time to send the packet [21]. According to this situation manage the packet to have the effective routing protocol.

Bounpadith Kannhavong, Abbas Jamalipour have proposed to detect the misbehavior node that drop topology control packets in OLSR. To do so, these nodes spoof links with the target’s two hop neighbors in order to gain Multi point relay position. This method send the TC message each node and an authentication acknowledgement back to the sender. In this scheme every relay node maintains a table containing its neighbor set of two hop information for their corresponding trust value.

Soufine Djahel, Farid Nait Abdesselam proposed a three hops acknowledgment based scheme to cope with the cooperative black hole attack in OLSR. In this scheme adds two extra packets to OLSR, Hello response packet which is a slight modification to Hello message and a small acknowledgement packet adding in the network

Alka chadhary, V.N.Tiwari, Anil Kumar have proposed a Detect packet dropping attack through malicious nodes in MANETs. The proposed solution is able to detect data dropping attack in distributed manner by each node and also remove the all malicious node [3]. Prevention based method such as authentication and encryption are not good solution, because all node contain public key for Adhoc networks to eliminate security threats.

Mohamed Elsalih Mahmoud and Xuemin shen have proposed the rational packet droppers to relay the other’s packets and enforce fairness and uses reputation system to identify and evict the irrational packet droppers [4]. Difficult to know trusted node or not in mechanism of finding whether the punishment mechanism.

Zehua Wang, Yuanzhu Chen, and Cheng Li have proposed a new loop-free proactive routing scheme for ODF in Mobile adhoc networks. PSR utilizes the hop count information as a metric to better explore the broadcast nature of the wireless medium, and enhance the efficiency and spatial use in opportunistic data forwarding [5]**.**

Zehua Wang, Yuanzhu Chen, and Cheng Li have proposed Proactive source Routing allows better control path selection by the source nodes for congestion avoidance, Load and energy consumption balancing, and energy consumption balancing. This protocol more control about the source node using the multiple receiver [6]. Future work improving the performance of PSR in the way that a data packet not dropped immediately after the link layer reports a transmission error.

Farid Nait Abdesselam, Soufine Djahel have proposed two scheme watchdog and path rater that aim to improve the throughput of network with the presence of misbehavior node . In this method find attack in fixed threshold based method. The main drawback of in this thresholdd method attack don't find distributed manner [7].

Akshai Aggarwal, Nirbhay chaubey, Keyurbhai A Jani have proposed designing an efficient and secure routing protocol is a daunting task. AODV is one of the widely researched on demanded routing protocol for use in MANETs [8]. Consider only limited number of node suppose take number of node high simulation difficult to understand.

Mohanapriya, Marimuthu and Ilango Krishnamurthi have proposed capable of finding whether a node is advertising correct topology information or not by verifying its Hello packets, thus identifyingmisbehavior node. Multipoint relay to provide efficient flooding mechanism by reducing the number of transmissions required. In OLSR (Optimized Link State Routing) protocol, two types of routing message are used HELLO message and TC (Topology Control) message. A HELLO message is the message that is used for Multi Point Relay and neighbor sensing. Topology control message contains the list of the sender's MPR selector.

ZehuaWang, Yuanzhu Chen, ChengLi have proposed proactive source routing protocol allows a node to have full path information to all other node in the network. Each node maintains a breath first search spanning tree of the network .PFA and LV were both originally proposed in this protocol, path finding algorithm based on distance vector and improves them by incorporating the predecessor of a destination in a routing update. In link vector algorithm reduces the overhead of link state algorithms to a great deal by only including links to be used in data forwarding in routing updates [9]. Here transmitter picks the best forwarder from more number of receivers, this receiver successfully received that data, and explicitly requests the selected node to forwarding data.

3. PROPOSED SYSTEM

Design and implement a new secured routing protocol to defense against packet dropping attack for PSR based protocol. The proposed system consists of packet dropping detection in Mobile Ad Hoc Network and also decreases the false negative rate even in the high mobility of nodes. Here used Two Ack send to the opposite direction in traffic of paths.

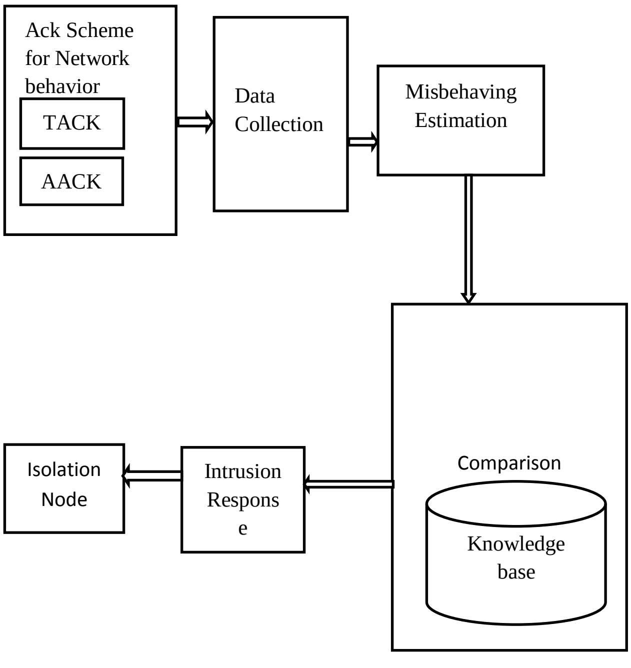

Fig 1: Overview of Proposed System

The detection techniques consists of two types that is point detection and intrusion detection, Here point detection is a single type of attack and intrusion detection system consists of range of attack. In the intrusion detection system can be monitoring the behavior of neighbor node and report to the sender. Proactive source routing protocol used to create the node topology and deep knowledge of each node present in that topology and perform both distance vector and link state routing. In this TWOACK based intrusion detection system consider the following parameters collision, heavy traffic in the media, overflow of transmission queue, Lack of energy resource, selfishness of a node and malignant act of a malicious node. In this situation the TWOACK based scheme accurate detection and report to the sender node, where is packet dropping happen. The most common method is to monitor the packet usage based on the watchdog and path rather scheme of wireless sensing packet dropping. However, all the existing approaches do not completely consider all the parameters (e.g., collision, heavy traffic in the media, and overflow of transmission queue) in Packet dropping.

Our proposed method used for proactive routing protocol, in this protocol contain knowledge about all node information. Acknowledgement scheme used to find, where packet dropping happen using packet dropping algorithm. After that collect the information using generation of trace file, in this trace file contain how many packet send and how many packet drop in each and every node. In this trace file information find the probability of misbehavior node in present network topology. Threshold value computing using counter method, in this counter method scheme used for time setting the before and after packet forwarding. Finally intrusion response to the senderside, how many packet drop and send in intermediate node.

ALGORITHM 1

```
---------------------------------------------------------------------------
Name: Received Packet in sender Side
Initial:$Count_{ack}$ ← 0, $Count_{pkt}$ ←0
Output: Counter Value
---------------------------------------------------------------------------
1.BEGIN
2.For each node
3.if (Received data packet) then
4. $Count_{pkt++}$
5.if (($Count_{ack}$<$Receive_{ack}$) then
6.Prepare MAC with $h_{i-1}$
7.Prepare $Seletive_{Ack}$ with ID, $h_i$
8.Send SeletiveAck
9.$Count_{ack++}$; //increase the counter of acknowledged packets
10.        End if
11.End for
12. END
```

ALGORITHM 2

Name: Received Packet in Detected Side

Initial: $Count_{ack} \leftarrow 0$, $Count_{pkt} \leftarrow 0$

Output: Counter Value

```
BEGIN
For each node
  While current time < Tstart+Tobs do
    if(forwarding data packet) then
      LIST ← LIST U dataID  //Add a data ID to LIST
      $Count_{pkts++}$ //Increase the counter of forwarded packets
          Setup timer ( r ) for data ID //Record the time
    end
    if(SACK packet received) then
          Search dataID carried by SACK from LIST
      if(found) then //A dataID received
          Check validity of $h_i$
        LIST ← LIST-dataID //Remove dataID from LIST
        Clear timer for ID
      end
    end
    if(timeout event happens)
      LIST← LIST – dataID //Remove dataID from LIST
      $Count_{mis++}$ // Misbehavior count increase
    end
    if($Count_{mis}$>$Receive_{mis}$) then //observation period expires
      Send link misbehavior report
END For
END
```

4. IMPLEMENTATION AND RESULTS

NS (Network Simulator) is an open source network simulation tool and discrete event driven simulator written in C++ and Otcl. Tool command Language (TCL) is front end of scripting language and C++ is back end C++ or Otcl.Network simulator (NS) is a simulation tool targeted at both wireless and wired networking in current networking research. NS is promising tool and is being used by universities and researchers.

Table Simulation Parameter

S.No	PARAMETERS	VALUE
1	Simulator	ns2.35
2	Radio Type	802.11b
3	Number of nodes	10,30,50
4	Traffic Type	TCP/UDP
5	Routing Protocol	DSDV/AODV
6	Number of Packets	512 bytes
7	No. of channels	One
8	Channel Frequency	2.4 GHz
9	Simulation Time	200 second
10	Simulation Area	1000m x 1000m
11	Mobility speeds	1 to 25 mps
12	Battery Model	Linear model

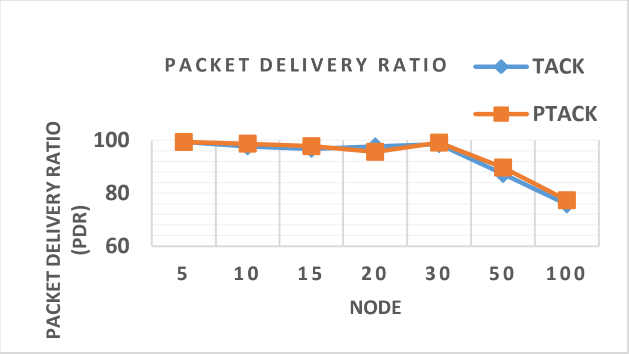

Fig.2. Simulation result for PDR in Proactive Protocol

The simulation result comparison between two routing protocol reactive and proactive routing protocol using acknowledgement based scheme. The proposed method modified AODV and DSDV protocol .First step to create the attack and check the performance of 5.10,15,20,30,50,100 node respectively.

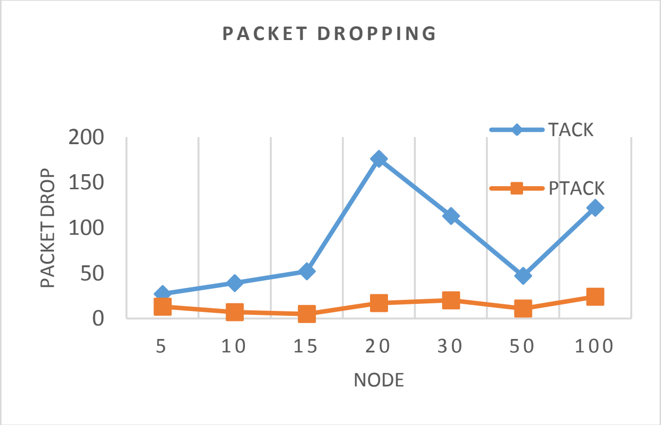

Fig.3: Simulation result for packet dropping in Proactive Protocol

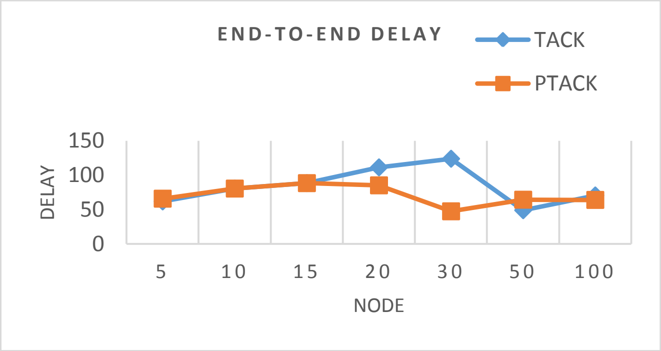

Fig.4: Simulation result for delay in Proactive Protocol

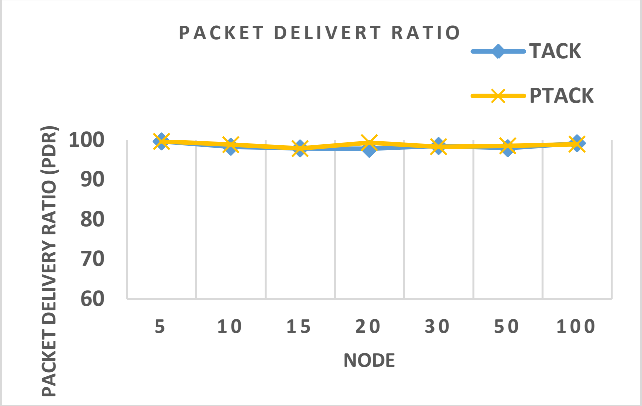

Fig.5: Simulation result for PDR in Reactive Protocol

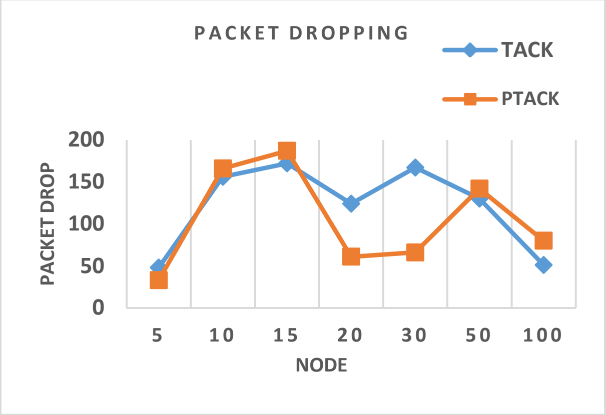

Fig.6: Simulation result for Packet dropping in Reactive Protocol

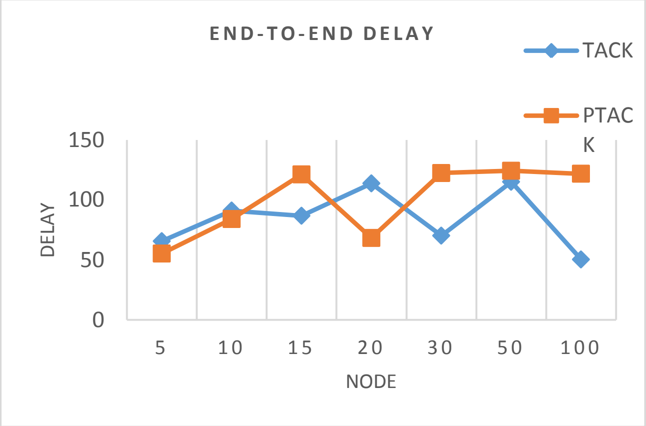

Fig.7: Simulation result for delay in Reactive Protocol

5. CONCLUSION AND FUTURE WORK

Mobile Adhoc Networks (MANETs) has been an lively research region over the earlier scarce years, due to their widespread submission in military and emergency process. But it communication to several types of attacks. Mischievousness of nodes may reason serve damage, smooth fails complete of the network. Proposed method will give an intrusion detection system to minimize packet dropping attack in MANETs, to give more security the network from the attack.The detection approach for dealing with selfish nodes. Selfish nodes are a real problem for adhoc networks since they affect the network throughput. Here used acknowledgement based method to detect the packet falling attack in Mobile Adhoc Network.In this method can be combined on highest of source routing procedure such Proactive Source Routing protocol and it is established acknowledgement packets for greeting of data packets on distribution and using immoral mode for counting the number of data packet such that it overcomes the problem of disobedient nodes.The future work will deals with how to prevention of packet dropping attack happen and includes certain authentication appliance to make positive that the Ack packets are not genuine and give suitable solution of this attack.

6. REFERENCE

[1] Adan Nadeem, Michael P. Howarth, “A Survey of MANET Intrusion Detection & Prevention Approaches for Network LayerAttacks”, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 4, FOURTH QUARTER 2013.

[2] Mrunal Pathak, Jyoti Hotte, “Survey On Acknowledgement Based Schemes For Misbehavior Detection In MANET”, International Journal of Advanced Computational Engineering and Networking, ISSN 2320-2106, Volume-2, Issue-4, April-2014.

[3] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, “EAACK- A Secure Intrusion-Detection System for MANETs”, IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013.

[4] Zehua Wang, Yuanzhu Chen, and Cheng Li, “PSR- A Lightweight Proactive Source Routing Protocol For Mobile Ad Hoc Networks”, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 63, NO. 2, FEBRUARY 2014.

[5] Kejun Liu, Jing Deng, Pramod K. Varshney, Fellow, Kashyap Balakrishnan, “An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs”, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 6, NO. 5, MAY 2007.

[6] Ziming Zhao, Hongxin Hu, Gail-Joon Ahn, Ruoyu Wu, “Risk-Aware Mitigation for MANET Routing Attacks”, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 2, MARCH/APRIL 2012.

[7] J.J. Garcia-Luna-Aceves, Fellow, IEEE, and Rolando Menchaca-Mendez, “STORM: A Framework for Integrated Routing, Scheduling, and Traffic Management in Ad Hoc Networks”, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 11, NO. 8, AUGUST 2012.

[8] Peng Zhang, Chuang Lin, Yixin Jiang, Yanfei Fan, and Xuemin (Sherman) Shen, “A Lightweight encryption Scheme for Network-Coded Mobile Ad Hoc Networks”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 9, SEPTEMBER 2014.

[9] Ze Li, Haiying Shen, “A QoS-Oriented Distributed Routing Protocol for Hybrid Wireless Networks”, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 3, MARCH 2014.

[10] Haiying Shen, Lianyu Zhao, “ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs”, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 6, JUNE 2013.

[11] Adnan Nadeem, Michael P. Howarth, “An intrusion detection & adaptive response mechanism for MANETs”, Elsevier, Ad Hoc Networks 13 (2014) 368–380.

[12] Wei Liu, Hiroki Nishiyama, Nirwan Ansari, Jie Yang, and Nei Kato, “Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 2, FEBRUARY 2013.

[13] Zhenzhi Qian, Xiaohua Tian, Xi Chen, Wentao Huang, and Xinbing Wang, “Multicast Capacity in MANET with Infrastructure Support”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 7, JULY 2014.

[14] Yang Qin, Dijiang Huang, and Bing Li, “STARS: A Statistical Traffic Pattern Discovery System for MANETs”, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 11, NO. 2, MARCH/APRIL 2014.

[15] Bingyang Liu, Jun Bi and Athanasios V. Vasilakos, “Toward Incentivizing Anti-Spoofing Deployment”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 3, MARCH 2014.

[16] Jinbei Zhang, Xinbing Wang, Xiaohua Tian, Yun Wang, Xiaoyu Chu, and Yu Cheng, “Optimal Multicast Capacity and Delay Tradeoffs in MANETs”, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 5, MAY 2014.

[17] Bin Tang, Baoliu Ye, Song Guo, Sanglu Lu and Dapeng Oliver Wu, “Order-Optimal Information Dissemination in MANETs via Network Coding”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 7, JULY 2014.

[18] Rossano Gaeta, Marco Grangett and Riccardo Loti, “Exploiting Rateless Codes and Belief Propagation to Infer Identity of Polluters in MANET”, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 7, JULY 2014

[19] Yaser khamayseh, Ruba Al-Salah, Muneer Bani Yassein, “Malicious Nodes Detection in MANETs: Behavioral Analysis Approach” , JOURNAL OF NETWORKS, VOL. 7, NO. 1, JANUARY 2012.

[20] Hoang Lan Nguyen , Uyen Trang Nguyen, “A study of different types of attacks on multicast in mobile ad hoc networks”, Ad Hoc Networks 6 (2008) 32–46.

[21] Ramasamy Murugan1 and Arumugam Shanmugam, “A Timer Based Acknowledgement Scheme for Node Misbehavior Detection and Isolation in MANET”, International Journal of Network Security, Vol.15, No.4, PP.241-247, July 2013.

[22] Anita, Abhilasha, “A Novel Technique to Protect and Isolate Selective Packet Drop Attack in MANET”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 6, June 2014.

[23] Qinli Wang, Guizhong Liu, “Network acknowledgement-based and error propagation-aware importance modelling for H.264/ AVC video transmission over wireless networks”, IET Commun., 2014, Vol. 8, Iss. 15, pp. 2737–2750.

[24] Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat, “Lightweight Sybil Attack Detection in MANETs”, IEEE SYSTEMS JOURNAL, VOL. 7, NO. 2, JUNE 2013.

[25] Aishwarya Sagar Anand Ukey, Meenu Chawla, “Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET”, IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 1, July 2010.

[26] S. Umang1 B.V.R. Reddy1 M.N. Hoda2, “Enhanced intrusion detection system for malicious node detection in ad hoc routing protocols using minimal energy consumption”, IET Communication Vol. 4, Iss. 17, pp. 2084–2094 - 2010.

[27] Zurina Mohd Hanapi1, Mahamod Ismail2, “Impact of blackhole and Sybil attacks on dynamic windows secured implicit geographic forwarding routing protocol”, IET Inf. Secur. Vol. 8, Iss. 2, pp. 80–87 2014.