IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 6, June 2016
ISSN (Online) 2348 – 7968 | Impact Factor (2015) - 4.332
www.ijiset.com

Implementation and Performance Analysis of Enhanced Adaptive Acknowledgment (EAACK) Protocol based on AODV

Jitendra Kumar Sharma[1], Ms. Bhawana[2] and Poonam Rani[3]

[1] M.Tech, Computer Science & Engineering, P M College of Engineering, Sonepat-131001, Haryana, India
[2] Assistant Professor,Computer Science & Engineering, P M College of Engineering, Sonepat-131001, Haryana, India
[3]Assistant Professor in Computer Science & Engineering, NSIT, Delhi, India

Abstract

MANET(Mobile Ad hoc network) is a collection of wireless mobile nodes forming a network without using and existing infrastructure.Compared to other network mobile ad hoc network is more vulnerable to various type of attacks.A new intrusion detection system is being designing for MANET's by the adoption of MRA(Misbehavior Report Authentication) scheme named as enhanced adaptive acknowledgement (EAACK) with ah-hoc on demand distance vector protocol(AODV).EAACK will be capable of detecting malicious nodes despite the existence of false misbehavior report and compared it against other popular mechanisms in different scenarios through simulation. The results will demonstrate positive performances against Watchdog, TWOACK and AACK in the cases of receiver collision, limited transmission power and false misbehavior report. EAACK demonstrates higher malicious behavior detection rates in certain circumstances while does not greatly affect the network performances. Due to some special function of Manets only prevention is not good for managing the secure networks. In this case detection should be focused as another part before an attacker can damage the structure of system.and result anamysiang based on packet delivery ratio(PDR) and Energy consumption.

Keywords: *MANETS,IDS, DSA, RSA, EAACK, AACK, TWOACK, IDS, MRA, S-ACK.*

1. Introduction

In the current age communication playing a very important role. Because of their improved technology and reduced cost wireless network is used over wired network. Mobile Ad-Hoc network is collection of mobile nodes. Mobile Ad-Hoc network can move anywhere anytime due to mobility feature. Mobile nodes equipped with both wireless transmitter and receiver communicates with each other.

MANET(Mobile ad-hoc network)[1] is vulnerable to various types of attacks because of dynamic network topology, lack of central administration and limited battery-based energy[1] of mobile nodes, open infrastructure. Several schemes had been proposed previously that solely aimed on detection and prevention of attacks. But most of these schemes become useless when the malicious nodes already entered the network or some nodes in the network are compromised by attacker. Such attacks are more dangerous as these are initiated from inside the network and because of this the first Defense line of network becomes ineffective. Since attacks are performed by participating malicious nodes which behave well before they are compromised therefore it becomes very difficult to detect.

In such case, Intrusion detection can be defined as a process of monitoring activities in a system which can be a computer or a network. The mechanism that performs this task is called an Intrusion Detection System (IDS)

Routing protocols are generally necessary for maintaining effective communication between distinct nodes. Routing protocol not only discovers network topology but also built the route for forwarding data packets and dynamically maintains routes between any pair of communicating nodes. Routing protocols are designed to adapt frequent changes in the network due to mobility of nodes. Several ad hoc routing protocols[2] have been proposed in literature and can be classified into proactive, reactive and hybrids protocols in fig 1.

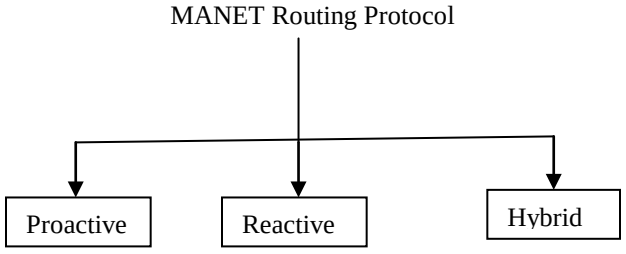

Fig 1: Manet routing Protocol classification

2. Security Attacks in MANET

There are various security issue[1] in MANET that can be classified as following.

1.Denial of Service Attack: This attack[4] aims to attack the availability of a node or the entire network. If the attack is successful the services will not be available. The

attacker generally uses radio signal jamming and the battery exhaustion method.

2. Impersonation: If the authentication mechanism is not properly implemented a malicious node can act as a genuine node and monitor the network traffic. It can also send fake routing packets, and gain access to some confidential information.

3.Eavesdropping: This is a passive attack[4]. The node simply observes the confidential information. This information can be later used by the malicious node. The secret information like location, public key, private key, password etc. can be fetched by eavesdropper.

4. Routing Attacks: The malicious node make routing services a target because it is an important service in MANETs. There are two flavors to this routing attack. One is attack on routing protocol and another is attack on packet forwarding or delivery mechanism. The first is aimed at blocking the propagation of routing information to a node.

5.Black-hole Attack: In this attack[3], an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it. A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packets that it receives instead of normally forwarding those packets.

6.Gray-hole Attack: This attack is also known as routing misbehavior attack which leads to dropping of messages. Gray whole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability.

7.Man- in- the- middle Attack: An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with receiver or impersonate the receiver.

8.Jamming: In jamming[3], attacker initially keep monitoring wireless medium in order to determine frequency at which destination node is receiving signal from sender. It then transmit signal on that frequency so that error free receptor is hindered.

9.Replay Attack: An attacker that performs a replay attack are retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to destroy poorly designed security solutions.

10. Wormhole Attack: In a wormhole attack[3], an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are tunneled. This tunnel between two colluding attacks is known as a wormhole.

3.Adhoc On Demand Distance Vector Routing(Aodv) Reactive Protocols

AODV discovers routes on an as needed basis via asimilar route discovery process. AODV[7] is a reactive protocol(routes are only generated on demand, in order to reduce routing loads). AODV is capable of both unicast and multicast routing. AODV uses sequence numbers to ensure the freshness of routes. It isloop-free, self-starting, and scales to large numbers of mobile nodes. However, AODV adopts every different mechanism to maintain routing information.It uses traditional routing table, one entry per destination.This is in contrast to dsr, which can maintain multipleroute cache entries for each destination. Without source routing, AODV relies on routing table entries to propagatean RREP back to the source and, subsequently, to routedata packets to the destination. AODV uses sequence numbers maintained at each destination to determinefreshness of routing information and to prevent routingloops. All routing packets carry these sequence numbers. An important feature of AODV is the maintenance oftimer-based states in each node, regarding utilization ofindividual routing table entries. A routing table entry is expired if not used recently. A set of predecessor nodes ismaintained for each routing table entry, indicating the set of neighbouring nodes which use that entry to route data Source node broadcasts a route request (RREQ) packet to its neighbors, which then forwards the request to their neighbors and so on. Fig 2 indicates the broadcast of RREQ across the network.

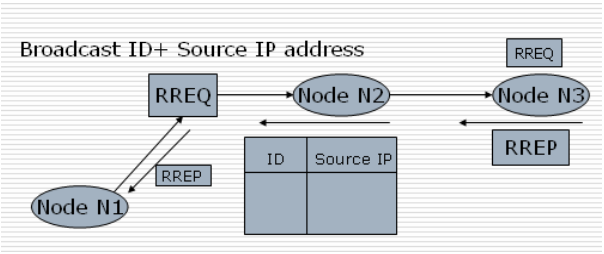

Fig 2. An illustration of AODV Protocol

3.1 Characteristics of AODV[6]

1. Unicast, Broadcast, and Multicast communication.
2. On-demand route establishment with small delay.
3. Multicast trees connecting group members maintained for lifetime of multicast group.
4. Link breakages in active routes efficiently repaired.
5. All routes are loop-free through use of sequence numbers.

6. Use of Sequence numbers to track accuracy of information.
7. Only keeps track of next hop for a route instead of the entire route.
8.Use of periodic HELLO messages to track neighbors.
9. Dynamic topology.

3.2 Advantages of AODV[5][7]

1.AODV is loop free and does not require any cartelized system to handle routing process for wireless mesh networks
2. The main advantage of AODV protocol is that routes are established on demand and destination sequence numbers are used to find the latest route to the destination.
3. The connection setup delay is less.
4.The HELLO messages supporting the routes maintenance are range-limited, so they do not cause unnecessary overhead in the network.
5.This protocol is reliable for the wireless mesh networks.

3.3 Disadvantages of AODV[5][7]

1. One of the disadvantages of this protocol is that intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries.
2. Multiple RouteReply packets in response to a single RouteRequest packet can lead to heavy control overhead.
3.Another disadvantage of AODV is that the periodic beaconing leads to unnecessary bandwidth consumption.
4. AODV do not utilize any congestion control or avoidance mechanism to balance traffic load.

4. PROPOSED WORK

An IDS collects activity information and then analyzes it to determine whether the rear any activities that violate the security rules. we have proposed a novel IDS named EAACK protocol specially designed for MANETs[10].

4.1 Existing System

4.1.1 Watchdog: The main of the watchdog[8] mechanism is to improve the throughput of the network with the presence of malicious nodes. The watchdog scheme is of two types namely watchdog and path-ratter. watchdog serve as intrusion detection for Mobile Ad-hoc Network and responsible for detecting malicious node misbehaviour in the network. Watchdog detects malicious node misbehaviours by promiscuously listening to its next hop's transmission. If a Watchdog node overhears that its next node fails to forward the packet within a predefined time period, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving.
At the same time, watchdog maintaining a buffer of recently sent packets and comparing each overheard packet With the packet in the buffer. A data packet is cleared from the buffer when the watchdog overhears the same packet being forwarded by the next-hop node over the medium. If a data packet remains in the buffer for too long, the watchdog scheme accuses the next-hop neighbour to be misbehaving as shown in fig 3.

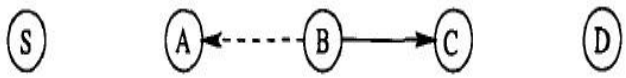

Fig 3: Working mechanism of watchdog

When B forwards a packet from S toward D through C, Node A cannot transmit all the way to node C, but it can listen in on node B's traffic. A can overhear B's transmission and can verify that B has attempted to pass the packet to C.
The solid line represents the intended direction of the packet sent by B to C, while the dashed line indicates that A is within transmission range of B and can overhear the packet transfer.
The path-ratter technique allows nodes to avoid the use of the misbehaving nodes in any future route selections. The routing information can be passed with the message. The Watchdog scheme fails to detect malicious misbehaviours with the presence of the following:

- Ambiguous collisions
- Receiver collisions
- Limited transmission power
- False misbehaviour report
- Collusion
- Partial dropping

4.1.2 Two ACK: with respect to six weaknesses in watch dog scheme several researches find out solution of these six weaknesses to solve these problems. TWO-ACK[9] schemes detects the misbehaving links by acknowledging each information packet transmitted over each three consecutive nodes from source to destination it is another important IDS to detect malicious nodes in the MANET. The main aim of these IDS is to solve the receiver collision problem and limited power transmission problem of watchdog. After receiving the packet each node has to send acknowledge packet to the node that is two hopes away from it down the route. Two ACK is required to work on the routing protocol such as dynamic source routing (DSR).
The operating method of TWOACK is shown in Fig 4: Node A primary forwards Packet 1 to node B, and then, node B forwards Packet 1 to node C. Once node C receives Packet 1, because it is two hops from node A, node C should send TWO-ACK packet, that contains reverse route from node A to node C, and sends it back to node A. The

IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 6, June 2016
ISSN (Online) 2348 – 7968 | Impact Factor (2015) - 4.332
www.ijiset.com

retrieval of this TWOACK packet at node A indicates that the transmission of packet one from node A to node C is fortunate. Otherwise, if this TWOACK packet is not received in an exceedingly predefined period, each nodes B and C area unit reported malicious. Identical method applies to each three consecutive nodes on the remainder of the route.Such process will degrade the life span of entire network[3].

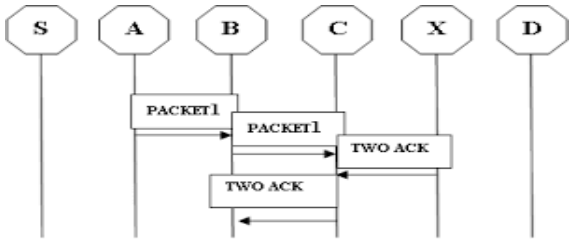

Fig 4: Two ACK

4.1.3 AACK: Adaptive acknowledgement (AACK)[10] is same as the two acknowledgements the difference is only that it provide end to end acknowledgement. As compared with two acknowledgements it reduces the network overhead still provides the identical network output. The end-to-end ACK IDS is shown in Fig. 5. The source node S sends out Packet 1 without any overhead. All the intermediate nodes simply forward this packet. When the destination node D receives Packet 1, it is required to send back an ACK acknowledgment packet to the source node S along the reverse order of the same path. Within a predefined time slot, if the source node S receives this ACK packet, then the packet transmission from node S to node D is successful. Otherwise, the source node S will switch to TACK (TWO ACK) IDS by sending out a TWO-ACK packet. The concept of adopting a hybrid IDS in AACK greatly reduces the network overhead, but both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehaviour report and fake ACK packets.

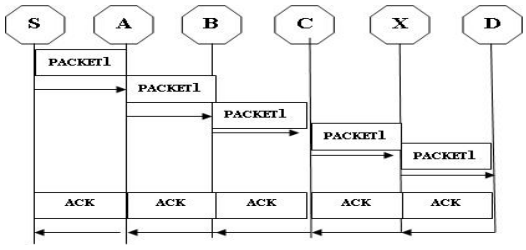

Fig.5 AACK

4.2 Problem Definition

(EAACK) Enhanced Adaptive Acknowledgement is design to solve the three of six weaknesses[11] of watchdog scheme namely.

1) Receiver collision
2) Limited transmission power
3) False misbehaviour.

4.2.1 Receiver collision: - As shown in the fig 6 once node A sends Packet1 to node B, it tries to take in if node B forwarded this packet to node C; in the meantime, node X is forwarding Packet2 to node C. In such case, node A overhears that node B has with success forwarded Packet 1 to node C however did not observe that node C is failed to receive this packet as a result of a collision between Packet 1 and Packet2 at node C.

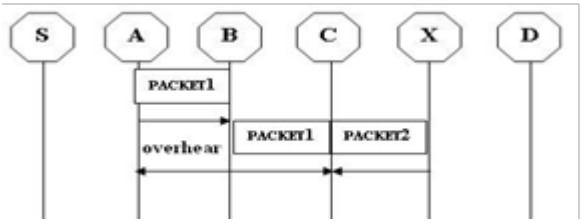

Fig.6 Receiver Collisions

4.2.2 Limited transmission power:- As shown in the fig7 of limited transmission power to manage battery resources node B limits its transmission power so that it is very strong to overheard by node A after transmitting power but it's too weak to reach at node C because transmission power is reduced at certain limit.

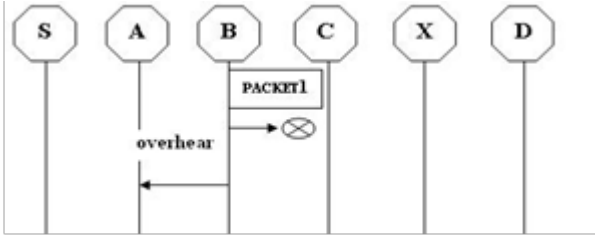

Fig.7 Limited Transmission Powers

4.2.3 **False misbehave :-** As shown in the fig 8 even though node A and node B send packet1 successfully to node C node A still inform node B as misbehaving due to open medium and remote distribution of typical MANETS. Attackers can add one or two nodes to achieve this false misbehaviour report attack. Two ACK and AACK can solve this problem of limited power transmission as well as receiver collision but both are fail to solve the problem of false misbehaviour attack. In order to solve receiver collision, limited transmission power as well as false misbehaviour attack the EAACK (enhanced adaptive acknowledgement) is introduced.

IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 6, June 2016
ISSN (Online) 2348 – 7968 | Impact Factor (2015) - 4.332
www.ijiset.com

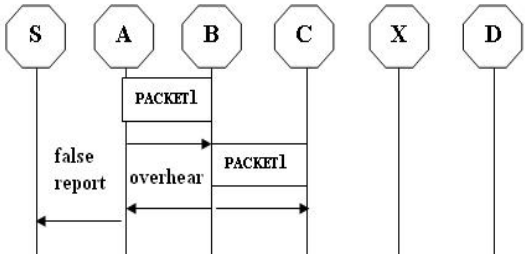

Fig 8 False Misbehave

4.3 Proposed Work

EAACK is consisting of three major part as acknowledgement (ACK), secure acknowledgement (S-ACK) and misbehaviour report authentication (MRA).

DATA	ACK	S-ACK	MRA

Fig 9 EAACK Protocol in MANET's

In these secure IDS, It is assumed that the link between each node in the network is bidirectional.Furthermore, for each communication process, both the source node and the destination node are not malicious. All acknowledgment packets are required to be digitally signed by its sender and verified by its receiver.

4.3.1. ACK: - ACK is basically an end-to-end ACK IDS. It acts as a part of the hybrid IDS in EAACK, Aiming to reduce network overhead when no network misbehaviour is detected. Consider the source node first sends out an ACK data packet to the destination node D. If all the intermediate nodes along the route between nodes S and D are cooperative and node D successfully receives packet, node D is required to send back an ACK acknowledgment packet along the same route but in a reverse order. Within a predefined time period, if node S receives packet, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

4.3.2. S-ACK: - It is an improved version of the TWOACK IDS. The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

4.3.3.MRA: - This field is designed to solve the problem of watch dog when it is fail to detect misbehaving nodes with the presence of false misbehaviour. False misbehaviour report may be able to generate by malicious attackers to falsely report innocent nodes as malicious. To initiate the MRA mode, the source node first searches its local knowledge base and seeks for an alternative route to the destination node. If there is no other route that exists, the source node starts a DSR routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes. When the destination node receives an MRA packet, it searches its local knowledge base and compares if the reported packet was received. If it is already received, then it is safe to conclude that this is a false misbehaviour report and whoever generated this report is marked as malicious. Otherwise, the misbehaviour report is trusted and accepted. By the adoption of MRA scheme. EAACK is capable of detecting malicious nodes despite the existence of false misbehaviour report.

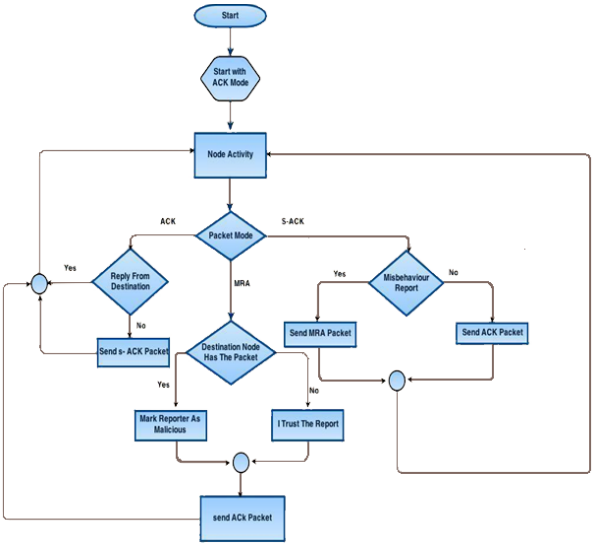

Fig 10. System Flow Of EAACK

5. Result:

I implement the EAACK protocol and Analyse result of EAACK based on packet delivery ratio and energy preservation.

5.1 Packet Delivery Ratio

PDR is the proportion of the total number of packets reached at destination and total number of packets send by the source. If the malicious packets increase PDR[21] also decrease gradually.

$$PDR = \frac{\text{Total number of data packet received (Receiver)}}{\text{Total Number of packets sent (Source)}}$$

5.2 Energy Consumption

I use the concept of the energy consumption. When I use number of nodes in MANET then how much energy is saved based on number of nodes. As the number of nodes will increase the more energy will be save and this also depend on the distance of the nodes. If the distance of the nodes that are communicating with each other is far then the less energy will be save.

5.3 PDR graph for Intrusion Detection

This graph show the result of the Intrusion Detection Based On PDR for different nodes.

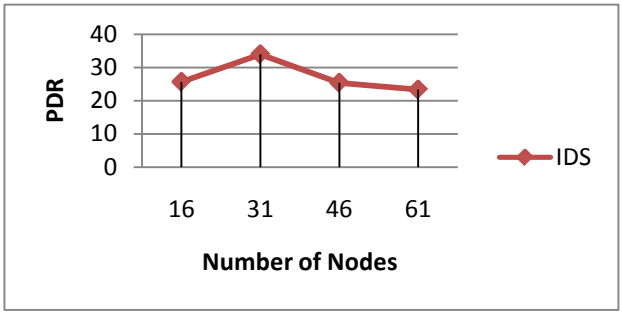

Fig 11: Intrusion Detection PDR graph

5.4 PDR graph for Intrusion Prevention

This graph show the result of the Intrusion Prevention Based On PDR for different nodes.

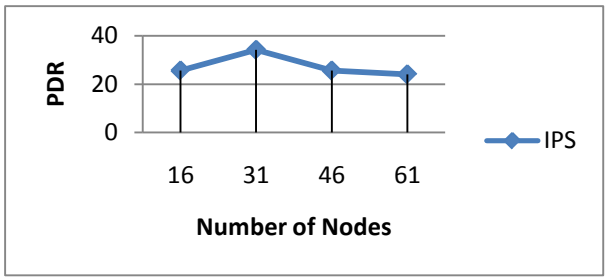

Fig 12: Intrusion Prevention PDR graph

5.5 Energy Consumption graph for Intrusion Detection

This graph show the result of the Intrusion Detection Based On Energy consumption.

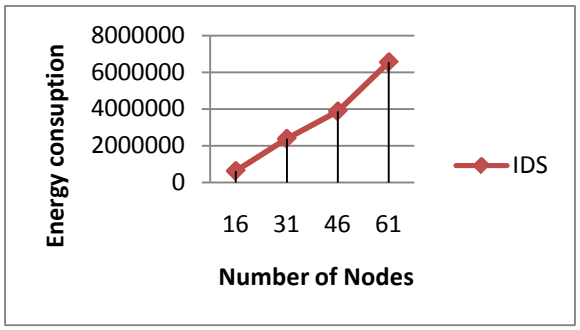

Fig 13: Intrusion Detection Energy Consumption graph

5.6Energy Consumption graph for Intrusion Prevention

This graph show the result of the Intrusion Prevention Based On Energy consumption.

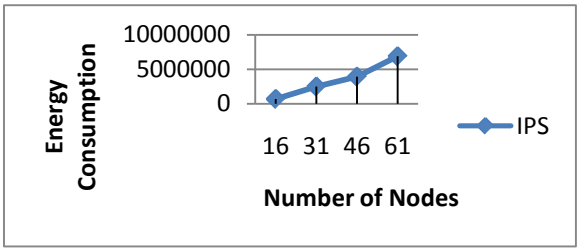

Fig 14: Intrusion Prevention Energy Consupmtion graph

6. Conclusions and Future work

6.1 Conclusion

I Implement the EAACK Protocol that solves the three weakness out of six weakness of the watch dog. These problems are receiver Collision, Limited transmission power and False Misbehave. I use the two parameter to comparison for the Intrusion detection and Intrusion Prevention based on the different- different nodes as 16, 31, 46 and 61. I use PDR(packet delivery ratio) and Energy Consumption In my work I apply the energy model for calculate the energy.Enrgy use between the transfer packet from source to destination node.

6.2 Future Work

In my research work I implement the EAACK protocol that solve the three problems of the watchdog as Receiver collision, Limited transmission power and False misbehaviour. In the future I will try to solve the remaining problems(Ambiguous collisions, Collusion,Partial dropping) of the watchdog so the Intrusion detection can be used properly to security purpose in MANET.

References

[1] V.Jayalakshmi, Dr. T. Abdul Razak ," *A Study on Issues and Challenges in Mobile Adhoc Networks*", International Journal of Innovative Research in Computer and Communication Engineering ,Vol. 3, Issue 9, September 2015.

[2]M. Dhatchayani, "*Wireless Sensor Network(WSN) Architectural Design and Applications*",International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 1, Jan-Feb 2014.

[3]Aarti and Dr. S. S. Tyagi,"*Study of MANET: Characteristics,Challenges, Applicati on and Security Attacks*", International Journal of Advanced Research in Computer Science and Software Engineering - Volume 3, Issue 5, May 2013.

[4] Anuj Rana, Sandeep Gupta ,"*Review on MANETs Characteristics, Challenges, Application and Security Attacks*", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013).

[5] **.** K.Sangeetha, *"Secure Data Transmission In Manets Using Aodv"*, International Journal of Computer & Communication Engineering Research (IJCCER) Volume2-Issue 1 January 2014.

[6] Nidhi Lal , "*An Effective Approach for Mobile ad hoc Network via I-Watchdog Protocol*" Indian Institute of Information Technology.

[7] Prashant Kumar Maurya, Gaurav Sharma, Vaishali Sahu, Ashish Roberts, Mahendra Srivastava, "*An Overview of AODV Routing Protocol*" , International Journal of Modern Engineering Research (IJMER) Vol.2, Issue.3, May - June 2012.

[8] Kiran Shinde , Prof. Harjeet Kaur ,Dr. Prakash Patil ," *EAACK —A Secure Intrusion-Detection System for MANETs*", International Journal of Electrical and Electronics Research, Vol. 3, Issue 1, pp: (97-102), Month: January - March 2015.

[9]K. Chinthanai chelvan, T. Sangeetha, V.Prabakaran and D.Saravanan "*EAACK-A Secure Intrusion Detection System for MANET*" International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 4, April 2014.

[10] G. Micheal and A.R. Arunachalam, "*EAACK: Enhanced Adaptive Acknowledgment for MANET*", Middle-East Journal of Scientific Research 19 (9): 1205-1208, 2014.

[11] Sarika M S , Hemanth S R ," *Eaack-A Secure Intrusion Detection System For Manets: A Survey*", International Journal For Technological Research In Engineering Volume 1, Issue 11, July-2014.