SRE-MAntNet routing protocol with IDS for SDA

Mr. Shivanna Jeeralabhavi[1], **Prof. Sherly Noel**[2]

[1]*M.Tech CNE, CMRIT Bangalore, VTU Belgaum, Karnataka, India.*
[2]*Asst. Professor, Dept. of CSE, CMRIT Bangalore, VTU Belgaum, Karnataka, India.*

---***---

Abstract - *In MANETs, nodes will have limited energy battery, it can deplete soon due to uncontrolled movement of nodes or if inefficient routing techniques are used. This may lead to collapse of whole network sometimes. A lot of research is going on since a decade to develop a routing protocol for MANETs which performs well with energy consumption, secured, reliable and provide IDS for crucial attacks. But we have observed research work focusing on one of these problems while developing the protocol. This paper proposes a routing mechanism which performs efficiently with respect all the above metrics. This paper proposes an ACO based routing scheme for MAntNet with aid to security, reliability, and efficient energy management technique. So this protocol is referred as SRE-MAntNet. It also proposes IDS for detection and prevention sleep deprivation attack which is quite common in MANETs. This follows a proactive routing approach and routing path is identified before initiation of data transfer. All these concepts are simulated through NS2, results are verified through demonstration of above mentioned concept and graphs are plotted for performance metrics such as Energy consumption, Throughput, bit error rate and packet delivery ratio. It is observed that proposed protocol outperforms with respect to all these metrics over existing E-MAntNet or E-AODV.*

Keywords → SRE-MAntNet, EAACK, S-ACK, SMA, IDS for Sleep deprivation attack.

1. Introduction

A group of independent mobile nodes communicating via radio waves constitutes a Mobile Ad-hoc Network (MANET). In the network, the nodes which are in radio range will communicate directly and which are out of range will communicate indirectly via intermediate nodes to route the packets. These nodes have inbuilt wireless interface for communication with each other. MANETs are fully distributed and can work with less or nil fixed infrastructure such as access points or base stations. The simple MANET consisting of 3 nodes would look like in Figure 1. Node 1 and 2 are within the range and hence direct communication is possible where as Node 1 and 3 are out of range from each other, hence the intermediate node 2 can be used for communication. The node 2 will act as a router here.

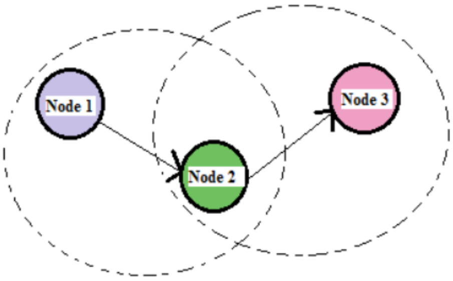


Fig. 1: MANET's Architecture

Usually MANETs are deployed in an area where less or almost nil man intervention is possible. So there won't be any proper infrastructure provided as base for it and also time constraint for deployment is too high in the situations like search and rescue, wars etc. Life time of MANETs is directly proportional to nodes energy. It is essential to have energy efficient routing protocol. As MANETs are deployed in remote areas, possibility of all forms of attack is high. So it is very important to have proper security mechanisms for secured data processing within and outside MANETs. Due to uncontrolled movement of nodes, high chances of route failures are possible. There should be a mechanism to detect dropped out packets and re-transmit them. It essential to have IDS for detecting various forms of attacks, one quite common attack in MANET is sleep deprivation attack.

2. Related work

In order to achieve the efficient routing over MANETs, the following concepts are cultivated according to requirements of the proposed system. At the micro-level, it mainly discusses on the concepts related to energy efficient routing scheme which is ACO based, security mechanisms through digital signature based authentication, reliability through EAACK-Enhanced Adaptive Acknowledgement and IDS for sleep deprivation attack.

1) Ant Colony Optimization: It is a technique to find the best path to the destination based on Ants nature. On the ground, it is found that the Ants are best ones to form efficient route between their nest and food source. The same is applied over the network to find the best routing path.

Double Bridge Experiment: This experiment is carried out by Mr. Deneubourg et al. to investigate the ants behavior and pheromone laying [1]. Here the nests of Argentine ants colony and food source were connected using two equal length bridges. In this type of settings, initially ants started the exploration of nest surroundings and try to reach the location of food by choosing one of the bridges randomly and deposit the pheromone. [2] After some time, higher concentration of pheromone is observed over one of the bridge due to random fluctuations and this path attracts more ants. This continues and eventually attracts whole colony ants to follow the same path. This colony level behavior of ants finds the shortest path between nest and food source in real-time.

The application of this ACO technique has grabbed huge attention of scientific community in recent past. [3] It works well in solving wide range of discrete optimization problems, problems raised while finding the dynamic shortest path in telecommunication networks, academic problems, industrial problems etc.

2) EAACK – Enhanced Adaptive Acknowledgement: In order make use of wireless medium advantages in MANETs, it is essential to have proper IDS for enhancing the security of MANETs [4]. If attack is detected with the help of IDS in the beginning only then it cannot cause much harm to the MANETs and also it can be recovered in most of the cases. We have found 3 such existing approaches explained in the below section.

a) Watchdog: This scheme is proposed by Mr. Marti et al. for improving the throughput of network with the presence of malicious nodes. This scheme consists of 2 parts namely watchdog and path partner. Main responsibility of Watchdog is to detect the harmful nodes. This fails when Receiver collisions, Ambiguous collisions, Limited transmission power, Collusion, False misbehavior report, Partial dropping.

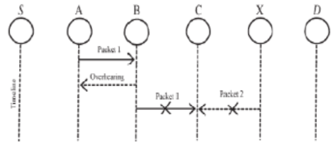


Fig. 2: Receiver Collision

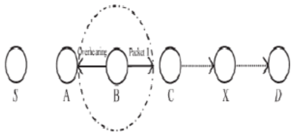


Fig. 3: Limited Transmission Power

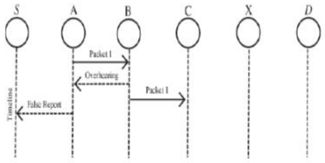


Fig. 4: False misbehavior report

b) TWOACK: In order to overcome the above mentioned watchdog scheme weaknesses, TWOACK scheme was proposed where in acknowledgment is expected on each and every packet transmission which leads into significant amount unnecessary traffic overhead. Hence it is not successful[5].

c) AACK: This is the new scheme proposed by Sheltamiet al. to overcome the drawbacks of TWOACK. AACK stands for adaptive acknowledgement and considered as network layer scheme. It is the combination of TWOACK and end-to-end ack schemes [5]. This scheme significantly reduces the overhead caused by TWOACK scheme but it still fail to detect the malicious nodes in presence of forged acknowledgement packets and false misbehavior report.

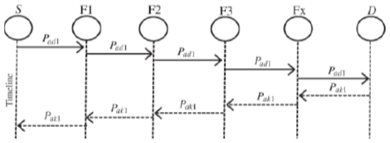


Fig. 5: ack scheme

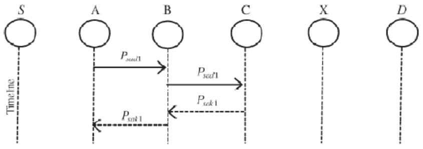


Fig. 6: Proposed S-Ack scheme

d) EAACK: This scheme is TWOACK's improved version and Liu et al. proposed this scheme. It is intended to group every three successive nodes and work together to identify malicious nodes. Once routing path is established, every 3rd node is expected to send intermediate ack to source called s-ack. Using this, misbehaving nodes can be detected even in presence of receiver collision or limited transmission power problems.

e) MRA: This is a new mode in EAACK scheme proposed to overcome the weakness of watchdog scheme to detect the node which can harm the network in presence of false misbehavior report [6]. In this scheme, destination node searches its local repository to find whether the packet mentioned in false misbehavior report is really missed like when destination node receives the MRA packet. If the packet reported is already received by the destination then it can be concluded that whichever node has sent this report as harmful else it is trusted and can be accepted

.

3) Digital Signature

Cryptography is the study of techniques required for achieving information security in terms of data confidentiality, integrity and authentication. The cryptography history originated way back from 4000 years in Egypt as per book published by Kahn in 1963.Digital signature plays vital role out of all available cryptographic techniques for authentication.

All the three techniques such as Watchdog, TWOACK and AACK used for authentication and reliability are vulnerable for attacks if the attackers are smart enough to forge the ack packets [7]. So application of digital signature to these ack packets would avoid forging of ack packets.

4) IDS for Sleep Deprivation Attack

Here Clusters are formed by grouping the Sensor nodes with sensor monitors as cluster head. IDS is executed in Sensor monitors.

An Illustrative Example of IDS using SMs

Consider the Figure-3.8, depicting topology of MANETs for [8] detection of sleep deprivation attack. It comprises of sensor monitors SM1-4, each sensor monitors covers the sensor nodes present in 1-hop radius. For eg. SM1 covers the sensor nodes 2, 8,17, 18 & 19.

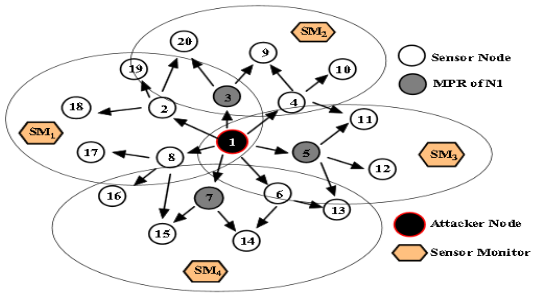


Fig. 7: Topology for Sleep deprivation attack

After the route discovery phase, best path is shared with sensor monitors. Each sensor monitors looks for the energy level of the node from its cluster participated in routing. If the energy level of routing node is less the max energy node within that cluster then there is a sleep deprivation attack and hence alternative route is formed via max energy node.

3. Proposed system

The main motto of this paper is to develop secured, reliable and energy efficient routing protocol with IDS for sleep deprivation attack and packet drop attack. Below is the proposed architecture at module level [5]. There are total 5 modules in our system and functioning of each of these modules is discussed in details below.

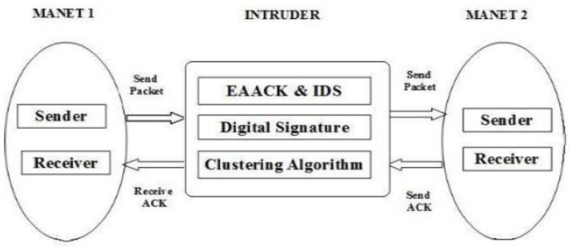


Fig. 8: Proposed System Architecture

3.1 Modules of Proposed System:

- Forward Ant Activities
- Backward Ant Activities
- EAACK
- Digital Signature Algorithm
- IDS for Sleep Deprivation Attack

1) Forward Ant Activities Algorithm:

This is the first step where routing path is discovered by ants to destination node based on transition probability base on energy levels of the path nodes and the algorithm involves the below tasks.

1. Source node generates the Ants at regular interval of time.

2. Next hop node selected based on equation (1) mentioned below (chose the highest energy neighbor with high percentage of pheromone). Here a forward hopping takes place to a node with a higher energy rather than with a shortest path length or with a node which takes less time in data transfer.

   The forward ant '*k*' choses to move to the next hop node 'Q' from '*S*' according to the below transition probability equation.

   $$P_K(Q) = \frac{[PH_Q]^{\alpha}\,[E_Q]^{\beta}}{\sum_{N \epsilon NEI}[PH_N]^{\alpha}\,[E_N]^{\beta}}$$

   ……………………. (1)

   Where *k* → Ant considered for checking node Q as next hop or not.

   N→ Node present in the neighbors NEI list.

   PHQ→ Node Q's Pheromone value

   EQ→Energy associated with node Q

   Alpha & *Beta* → Weights associated with Pheromone and Energy of nodes.

   Note - Pheromone value of node changes every time it is selected as next hop.

3. Pheromone value gets calculated and updated in routing table after forward ant passes through each node. Usually it updates the metrics like hop count, time elapsed, Energy, Pheromone on the traversed node etc.

4. Forward ant gets converted into backward ant on reaching the destination and traverses back according the routing path identified.

   Pheromone update rule: DeltaPHk is the pheromone value added to the existing value of node Q (*PHQ*) when backward Ant crosses the node Q on its backward journey.

$$\Delta PH_k = 1/(C - E_{avg}) \qquad \text{........................ (2)}$$

Where C →initial energy assigned to nodes

Eavg → Networks average at that timestamp.

Evaporation of Pheromone rule: Once Ant gets transitioned into next hop node Q, , evaporation of pheromone of Q is given by

$$PH_Q = PH_Q - PH_Q * \rho \qquad \text{..................... (3)}$$

Where ρ →evaporation factor

Finally the pheromone value updated by backward ant is given by

$$PH_Q = PH_Q * (1-\rho) + \Delta PH_k \qquad \text{............. (4)}$$

2) Backward Ant Activities Algorithm:

1. Backward ant starts its journey towards source according to the routing info stored identified by forward ant.
2. Pheromone trial '*DeltaPHQ*' to be deposited along the path by the ant 'k' is calculated by destination node as per Eq. (2)
3. *Backward Ant k deposits 'DeltaPHQ'* of Pheromone in the routing table of the node it traverses.
4. Intermediate node '*Q*' updates *PHQ* obtained from Eq. 4 in its routing table.
5. On reaching source, backward ant will be dropped and data transfer initiated.

Flowchart for forward and backward ant activities implementation is shown below.

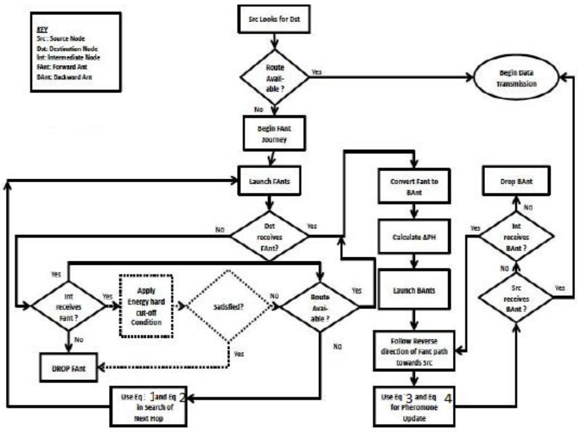


Fig. 9: Flow chart for SRE-MAntNet route discovery process

3) EAACK – Enhanced Adaptive Acknowledgement

This is the module deals with reliable packet transfer, 2 ways adaptive acknowledgement approaches is followed here.

Approach 1. Every 3rd node involved in routing will send the secured acknowledgement (s-ack) to the source node. This approach ensures the identification of packet drop and re-transmits.

Approach 2. Once data packets reached destination node, it will send the **ack** packet to the source for final confirmation.

4) Digital Signature Algorithm

Three IDS schemes such as Watchdog, TWOACK and AACK will fail if the attackers are too smart to forge the ack packets. Hence digital signature based authentication is used to exchange the ack packets in EAACK technique. This algorithm makes the system to operate in 3 modes, ack, s-ack and MRA mode. The first two modes implementation is already explained in previous section and 3rd mode is used for re-transmitting the dropped packets.

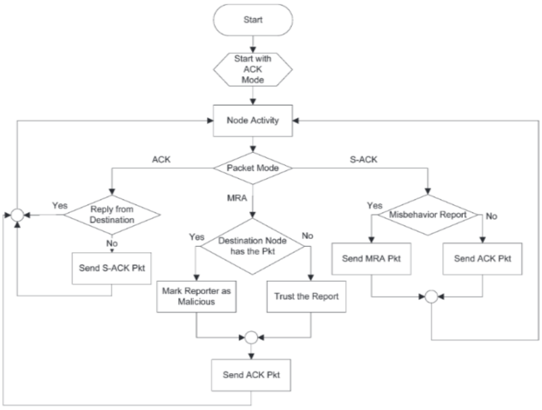


Fig. 10: Flow chart for EAACK

5) IDS for Sleep Deprivation Attack

This is the critical and common type of attack in MANETs. In this form of attack, attacker targets nodes which are having less energy. So we have followed the cluster based approach to detect the compromised node and select the alternative node from the cluster which has the max energy in that cluster to form the alternate routing path.

Algorithmic steps:

1. Formation of clusters in the MANET
2. Introduce sensor monitors which work as cluster heads
3. SM will identify the Max energy node from the cluster
4. SM will fetch the details of the node participated in routing from its cluster
5. Compare the energy level of routing node and Max energy of cluster.
6. Drop the routing node if its energy is less than the max energy.
7. Set up alternate routing path through the Max energy node of the cluster.

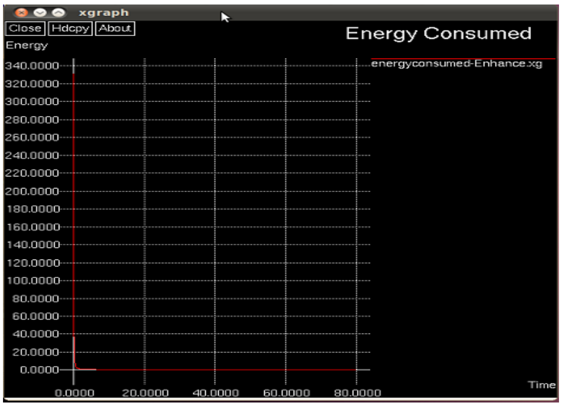
3.2 Advantages of proposed system:

- Secured routing using EAACK.
- Reliable packet transfer using digital signature for authentication
- Minimized packet drop ratio and retransmission mechanisms in case of drop
- Provides IDS for detection and Prevention of Sleep deprivation attack which is a serious form of attack in MANETs.
- Enhanced life time of MANET due to energy aware version.

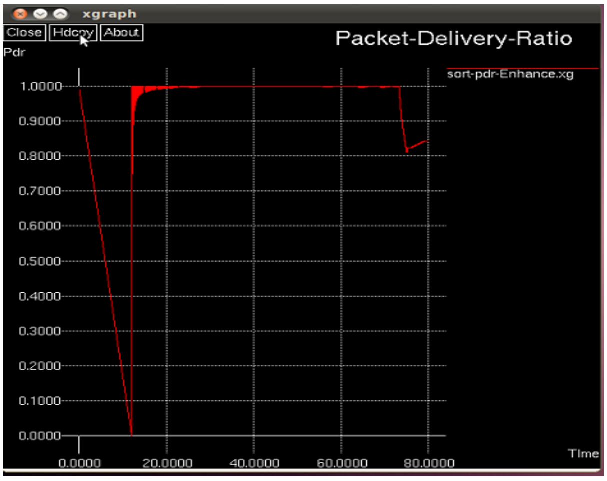
4. RESULTS

a) Proposed (SRE-MAntNet) Protocol graphs

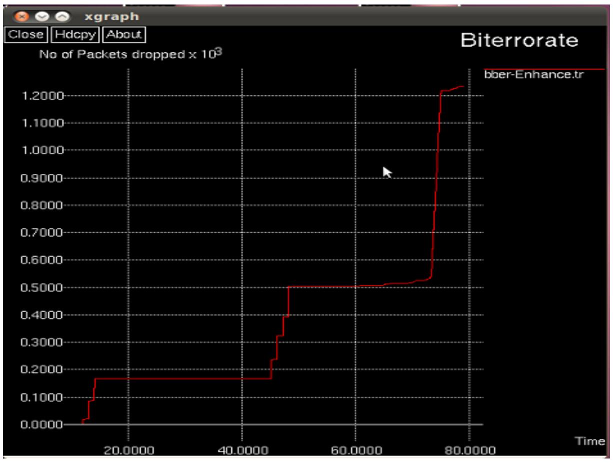
1. Energy Consumption



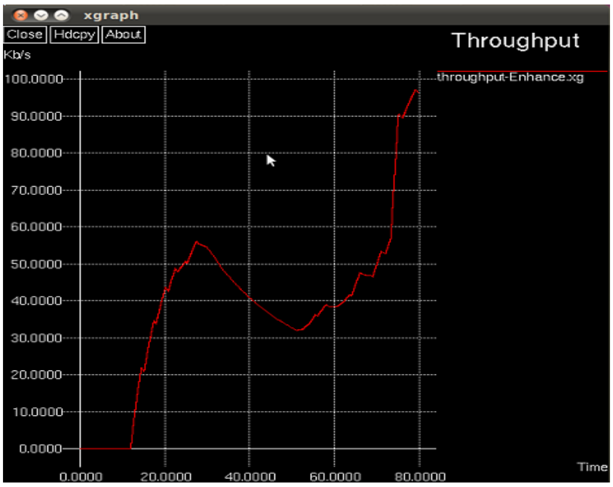
2. Packet Delivery Ratio



3. Bit Error Rate

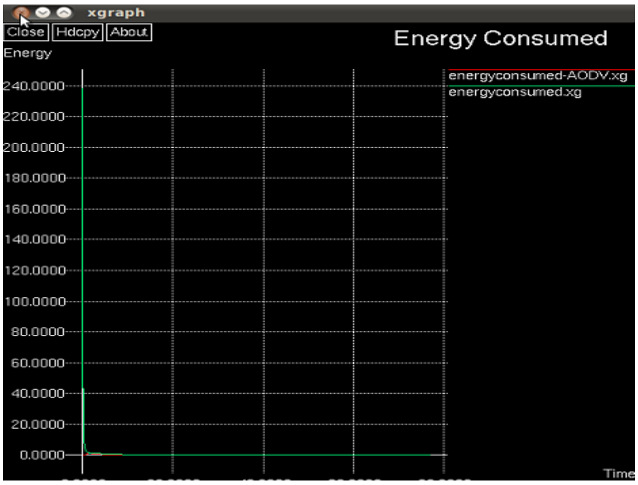


4. Throughput

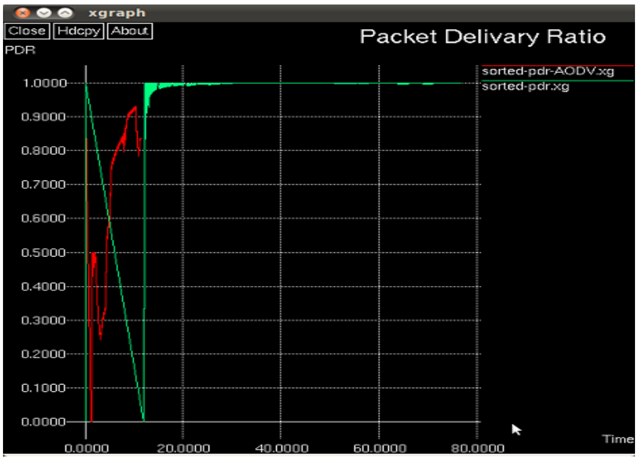


b) Existing (E-AODV) protocol graphs

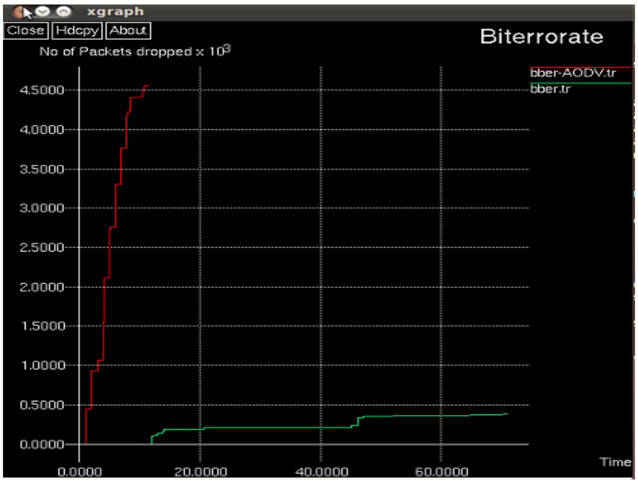
1. Energy Consumption



2. Packet Delivery Ratio



3. Bit Error Rate



4. Throughput

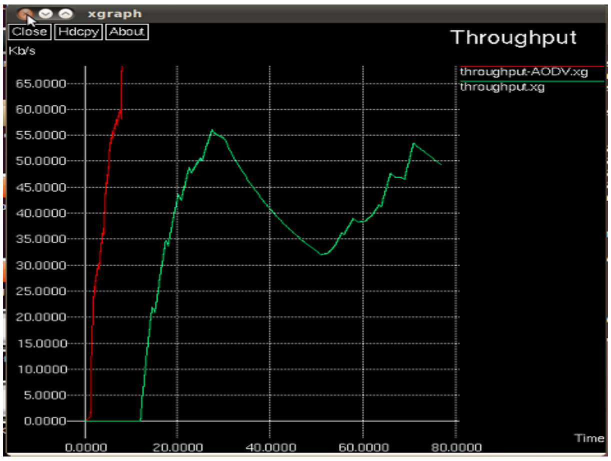


Fig. 10: Graphical of results

5. CONCLUSION AND FUTURE SCOPE

All of the work explained above related to ACO based routing path set up mechanism, EAACK, Digital signature and IDS for prevention of Sleep deprivation attack are extensively simulated through NS2 tools and compared the performance behavior of proposed protocol over existing protocols like AODV, MAntNet. It is observed that the 20-30% overall performance improvement in terms of energy consumption, packet delivery ratio, throughput and bit error rate over existing routing protocols like AODV, MAntNet.

We intended to develop stronger IDS system which can address other forms of attacks and also address the mobility issues in more passionate way.

REFERENCES

[1]. Anuj K Gupta, Harsh Sadawarti and Anil K. Verma, *"Computation of Pheromone Values in AntNet Algorithm". International Journal of Computer Network & Information Security*, vol. 4, no. 9, pp. 47-54, 2012.

[2]. A Radwan, T Mahmoud and E. Houssein, *"AntNet-RSLR: a proposed ant routing protocol for MANET". Proceedings of the first Saudi international electronics, communications and electronics conference (SIECPC'11)*, pp. 1-6.

[3]. Ssowjanya HariShankar, Isaac Woungang, Sanjay Kumar Dhurandher, Issa Traore, Shakira Banu Kaleel, *" E-MAntNet: An ACO-Based Energy Efficient Routing Protocol for Mobile Ad Hoc Networks"*. 2015 IEEE 29th International Conference on Advanced Information Networking and Applications.

[4]. T.Archana, Mr.N.Rajkumar, *" Enhanced Acknowledgement Based Intrusion Detection for Manets"*. ISBN No.978-1-4799-3834-6/14/$31.00©2014 IEEE

[5]. A Al-Roubaiey, T. Sheltami, A. Mahmoud, E. Shakshuki, H. Mouftah, *" AACK: Adaptive Acknowledgment Intrusion*

Detection for MANET with Node Detection Enhancement''. 2010 24th IEEE International Conference on Advanced Information Networking and Applications.

[6]. Deore Suvarna, Erande Pallavi, Lahane Sumitra, Dhatrak Chhaya, Prof. Mahesh Korade, *''Acknowledgement security for MANET using EAACK''*. 978-1-4673-7910-6/15/$31.00_c 2015 IEEE.

[7]. BAI Qing-hai, ZHANG Wen-bo, JIANG Peng, LU Xu, *'' Research on Design Principles of Elliptic Curve Public Key cryptography and Its Implementation''.* 978-0-7695-4719-0/12 $26.00 © 2012 IEEE, DOI 10.1109/CSSS.2012.310.

[8]. Chaitali Biswas Dutta, Utpal Biswa, *''Intrusion Detection System for Power-Aware OLSR''*. 2015 International Conference on Computational Intelligence & Netwlorks.