Grenze International Journal of Engineering and Technology, June Issue

Optimal Trust based Hybrid Collaborative Path Tracing System for Defending Black Hole Attack in MANET

Dr. S. Vadhana Kumari[1] and Dr. A. Sherly Alphonse[2]
[1]Ilahia College of Engineering and Technology, Department of Computer Science and Engineering
Mulavoor, Kerala, India
E-mail: vadhanakumari@icet.ac.in
[2]Vellore Institute of Technology, SCOPE, Chennai, Tamil Nadu, India
E-mail: sherly.a@vit.ac.in

***Abstract*—Mobile Ad-hoc network (MANET) is an infrastructure less network where communication takes place between collections of mobile hosts. There are several threats to ad-hoc network termed popularly as active and passive attacks. Collaborative attack is a new generation threat for ad-hoc networks. In collaboration Black hole attacks, multiple attackers synchronize their actions against some network to disturb the genuine communication. This paper proposes a new technique called Optimal Trust Based Hybrid Collaborative Path Tracing System for defending Black hole Attack in MANET by finding out dubious path information from black hole nodes. Also, a Swarm based optimal trust inference model is introduced to compute the trust of each node and therefore, the data encrypted using AES algorithm can be forwarded through these trusted nodes. Experimental results assessed using NS2 simulator show that in the presence of malicious nodes, the proposed system works better than the existing techniques in terms of routing overhead and packet delivery ratio.**

***Index Terms*— MANET, Collaborative, Path Tracing, Black-hole attack, dubious path, Encryption.**

I. INTRODUCTION

Mobile ad hoc networks (MANET) [1] have no network infrastructure and hence, a node must relay packets to its neighbor nodes for network connectivity. Early research work on route establishment in MANET has mainly focused on the probability and efficiency of packet delivery [2] [3], assuming that nodes are trustworthy and cooperative. Due to the widespread availability of mobile devices, mobile ad hoc network is widely used for various important applications such as military crisis operations, emergency preparedness and response operations. This is primarily due to their infrastructure less property. In MANET, each node not only works as a host but also acts as a router [4]. While receiving data, nodes need to cooperate with each other to forward the data packets, thereby forming a wireless local area network. The presence of malicious nodes in the network may disrupt the routing process, leading to malfunctioning of network operations [5]. The lack of any infrastructure added with the dynamic topology feature of MANETs make these networks highly vulnerable to routing attacks such as black hole and gray hole All intermediate nodes between the source and destination take part in routing, also called hop-by-hop communications [6]. Due to these characteristics, each node can easily gain access to other node's packets or inject fault packets to the network. Therefore, securing MANET against malicious nodes

Grenze ID: 01.GIJET.8.2.507_2

became one of the most important challenges. [7]-[9].The aim of this paper is to provide a brief discussion and analysis on black hole in MANET. In black hole attacks, a node transmits a malicious broadcast message informing that it has the shortest path to the destination with the goal of intercepting messages. In this case, a malicious node can attract all packets by using forged Route Reply (RREP) packet to falsely claim the "fake" shortest route to the destination and then discard these packets without forwarding them to the destination. It then selectively discards/forwards the data packets when they go through it [10]. The remainder of the paper is organized as follows: Section 2 provides the discussion of recent related works; Section 3 illustrates the problem methodology and system model of proposed HCPT. Section 4 describes the working function of the proposed work and the performance comparison is discussed in Section 5. Finally, the paper concludes in Section 6.

II. Related Works

Tsou et al. [11] proposed a technique to forward the data packets by designing a dynamic source routing (DSR)-based routing mechanism, which is referred to as the cooperative bait detection scheme. It integrates advantages of both proactive and reactive defense architectures. This method implements a reverse tracing technique which helps to detect malicious nodes in MANETs under gray/collaborative black-hole attacks. But routing overhead and packet delivery ratio is considerably not a reasonable one.

Baadache et al. [12] proposed a secure mechanism for checking the good forwarding of packets by an intermediate node. This solution is based on the principle of Merkle tree in which each leaf carries a given value and the value of an interior node. It enables each node to generate its secret and communicates the root value of the Merkle tree to the transmitter node. Here each node,i, generates a secret key which is independent of others. So it will prevent another node to replay the role of the node i, but creating a very large network of merkle tree is difficult.

Marti et al. [13] proposed two techniques to improve the throughput in an ad hoc network in the presence of nodes that agree to forward packets but fail to do so. To mitigate this problem we use a watchdog that identifies misbehaving nodes and a path ratter that helps routing protocols avoid these nodes .But, both techniques are more time consuming.

Liu et al. [14] proposed a 2ACK scheme for the detection of routing misbehaviour in MANETs. In this scheme, two-hop acknowledgement packets are sent in the opposite direction of the routing path to indicate that the data packets have been successfully received. A parameter acknowledgment ratio, i.e., Rack, is also used to control the ratio of the received data packets for which the acknowledgment is required. This scheme belongs to a class of proactive schemes and, hence, produces additional routing overhead regardless of the existence of malicious nodes.

Vishnu et al. [15] proposed a mechanism for the detection of black hole attack by using Core Maintenance of the Allocation Table. In this approach, only the backbone network in MANET is permitted to select the IP addresses for unconfigured hosts. This mechanism is based on allocating a conflict free address to all newly arrived nodes using multiple disjoint address spaces. Each backbone node (BBN) in MANET is responsible for allocating a range of addresses disjoint from the ranges of all other BBN. In other words, each BBN generates numbers that are unique for that host. Every hosts in the MANET must have the possibility to reach one of the BBN at any time. If the Source Node (SN) gets an RREP for the RIP (Restricted IP), then there is a black hole in that route. In this case, the SN initiates the process of Black Hole detection. The SN initially alerts the neighbors of the node from which it received the RREP to RIP, to enter into promiscuous mode for tracing the black hole node. Routing Overhead is high in this proactive detection scheme.

Nygard et al. [16] proposed a methodology for identifying multiple black hole nodes cooperating as a group with slightly modified AODV protocol by introducing Data Routing Information (DRI) Table and Cross Checking. In this technique each node maintain additional DRI table. Source node performs cross checking of the Replied Node by using DRI information from the Next Hop Node. However, this additional DRI table causes increased overload.

III. Problem Methodology and System Model

A. Problem methodology

Security needs are Higher in MANET compared to the traditional network. Hence, there is a need for a comprehensive security solution which can deal with various types of attacks. As such, it can identify all the addresses of nodes in the selected routing path from source to destination. However, the source node may not necessary be able to identify which of the intermediate nodes has the routing information to the destination. This scenario may result in having the source node sending its packets through the fake shortest path chosen by the

malicious node, which may then lead to a black hole attack. The Hybrid Collaborative Path Tracing system (HCPT) effectively finds out the dubious path information from black hole node.
The main contributions of proposed HCPT as follows:

- Find out the dubious path information from black hole node.
- Using Swarm based optimal trust inference model to compute the trust of each node.
- Using AES encryption technique to encrypt the data and forward it through the trusted nodes.

B. System model of proposed HCPT

Fig. 1 shows a scenario of a network having a black hole node BH. The source node SN starts the route discovery process by broadcasting RREQ packet in the network in order to find the routes for destination node DN. The RREQ packets broadcasted by SN are then received by the neighboring nodes. When the black hole node i.e. BH node, gets the RREQ packet, it quickly responds with a fake RREP packet without considering its own routing table for any routes towards DN. As the reply packet from BH node contains the highest sequence number for DN, the source node immediately considers it and updates its routing table for the route towards malicious node and discards all the other RREP packets, even the reply packet from DN also. Once SN selects the path through node 3, it forwards the data packets towards black hole node for the intended destination node. As per the nature of black hole node, it throws all the data packets away, rather than sending it towards next hop nodes.

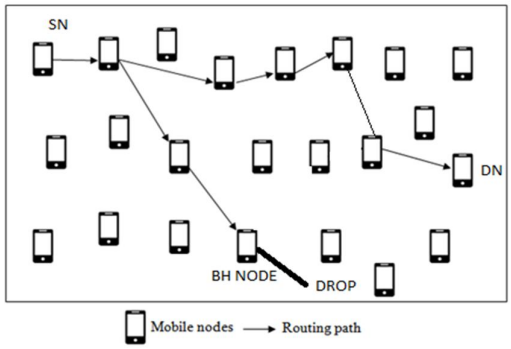

Figure 1. Network Model – Detection of Black Hole Node

IV. Proposed Hybrid Collaborative Path Tracing System (HCPT)

A. Algorithm for Detection of Black hole node using path tracing technique.

Algorithm 1: Black hole attack detection using HCPT technique.

1. Source Node selects an address of adjacent node as fake destination address to generate fake Route request and sends it to intermediate nodes.
2. If the route reply is from true destination then there is no malicious attack.
3. Otherwise Source node starts to find out the dubious path information from black hole node.
4. Using Swarm based optimal trust inference model to compute the trust of each node.
5. Using AES encryption technique to encrypt the data.
6. Forward the encrypted data through that trusted nodes.

B. Find out the dubious path information from black hole node.

The malicious node has received the RREQ, it will reply with a false RREP. When a malicious node, for example, mn, replies with a false RREP by generating fake address list, $P = \{n_1, \ldots n_k, \ldots n_m, \ldots n_r\}$ which is recorded in the RREP. If node n_k receives the RREP, it will separate the P list by the destination address n_1 of the RREP in the IP field and gets the address list $K_k = \{n_1, \ldots n_k\}$, where K_k represents the route information from source node n_1 to destination node n_k. Then, node n_k will determine the differences between the address list $P = \{n_1, \ldots n_k, \ldots n_m, \ldots n_r\}$ recorded in the RREP and $K_k = \{n_1, \ldots n_k\}$. Consequently, we get $K'_k = P - K_k = \{n_{k+1}. \ldots n_m, \ldots n_r\}$, where K'_k represents the route information to the destination node (recorded after node n_k). The operation result of K'_k is stored in the RREP's "Reserved field" and then reverted to the source node. Each node in the same route which receives the RREP will do this same operation and the dubious path information DP replied by malicious nodes could be detected, i.e.,

$$DP = K'_1 \cap K'_2 \cap K'_3 \ldots \cap K'_k. \quad (1)$$

Given that a malicious node would reply the RREP to every RREQ, nodes that are present in a route before this action happens are assumed to be trusted. The set difference operation of P and DP is conducted to acquire a temporarily trusted set T, i.e.,

$$T = P - DP \quad (2)$$

C. Trust computation using Swarm based optimal trust inference model

The proposed trust computation model is inspired from the Swarm algorithm. It modifies the Swarm algorithm to solve global optimization problems which is mainly based on the foraging strategy of social spiders, utilizing the vibrations on the spider web to determine the position of the victim. This algorithm emulates this behavior of social spiders to perform optimization. The solution of optimization problem is to find the position of spiders through spider searching space that is responsible for translating the information between spiders. The communication between the spiders is performed using vibration that transmitted when the spiders move to a new position. The vibration between spider a_i and a_j is generated by the weight and position of a_j as follows:

$$V_{a_{i,j}} = \upsilon_{a_j} e^{-d^2_{a_{i,j}}}; \qquad d_{a_{i,j}} = \left\| a_i - a_j \right\| \quad (3)$$

Where υ_{a_j} is the weight of the spider a_j defined as follows:

$$\upsilon_{a_j} = \frac{FF(a_j) - W_a}{B_a - W_a} \quad (4)$$

Here, $FF(a_j)$ is the fitness function value obtained by evaluation of a_j, and the W_a, B_a is the worst and best case respectively as follows:

$$W_a = \min_{k=1,\ldots,k} FF(a_k) \quad (5)$$

$$B_a = \max_{k=1,\ldots,k} FF(a_k) \quad (6)$$

There are two strategies to update the position of spiders depending on their gender - males and females (the females represent 60–90% from the total number of spiders). The female spider updates its position as follows

$$X^{k}_{FM_{a_i}} = \begin{cases} X^{k}_{FM_{a_i}} + r_1 \times \upsilon_{a_1} \times \left(a_1 - X^{k}_{FM_{a_i}}\right) + r_2 \times \upsilon_{a_2} \times \left(a_2 - X^{k}_{FM_{a_i}}\right) + r_3 \times (\xi - 0.5); & Random \geq M \\ X^{k}_{FM_{a_i}} - r_1 \times \upsilon_{a_1} \times \left(a_1 - X^{k}_{FM_{a_i}}\right) - r_2 \times \upsilon_{a_2} \times \left(a_2 - X^{k}_{FM_{a_i}}\right) - r_3 \times (\xi - 0.5); & Otherwise \end{cases} \quad (7)$$

Where r_1, r_2, r_3, $Random$ and ξ are random numbers between (0, 1), M is threshold value to move the spider toward or away from the source of vibration and k represents the number of iterations. The individual a_1 represents the nearest spider to a_i that holds a higher weight, and a_2 is the best individual. υ_{a_2} is the vibration transmitted by the best spider a_2 and its corresponding weight and position is represent as follows:

$$\upsilon_{a_2} = W_{a_2} e^{-d^2_{a_{i,2}}}; \qquad W_{a_2} = \max_{k=1,\ldots,k} W(a_k) \quad (8)$$

The υ_{a_i} is the vibration transmitted by the nearest spider that has the best weight represented as follows:

$$\upsilon_{a_1} = W_{a_1} e^{-d^2_{a_{i,1}}}; \qquad W_{a_1} > W_{a_i} \quad (9)$$

If the female concentrates to move towards the source of vibrations, the first condition of equation (4) is used, otherwise the second condition is used. The male spiders update their position based on whether male is domineer or non-domineer, where non-domineer spiders are attracted toward females spiders; whereas the domineer spiders tend to move towards the center of the male population to become domineer males. The males update their position as follows:

$$X^{k+1}_{M_{a_i}} = \begin{cases} X^{k}_{M_{a_i}} + r_1 \times \upsilon_{a_3} \times \left(a_3 - X^{k}_{M_{a_i}}\right) + r_3 \times (\xi - 0.5); & W_{M_{a_i}} \geq W_{median} \\ X^{k}_{M_{ai}} + r_1 \left(\left(\sum_{a_{j=1}}^{M_n} X^{k}_{M_{a_i}} \cdot \frac{W_{a_3+j}}{\sum_{a_{j=1}}^{M_n} W_{a_3+j}} \right) - X^{k}_{M_{a_i}} \right); & Otherwise \end{cases} \quad (10)$$

where M_n is the number of male spiders and W_{median} is median of weight of all male spiders. If the weight value of male spider is greater than W_{median} then it is considered as dominant, otherwise, non-dominant.

The spider a_3 is the closest female to i^{th} male, and υ_{a_3} is the vibration transmitted by the nearest female and it is defined as:

$$V_{a_3} = W_{a_3} . e^{-d^2_{i,a_3}} \tag{11}$$

The final step of the algorithm is mating between the females and dominant male spider on the neighbor with mating radius defined as follows:

$$M_{F,DM} = \frac{\sum_{a_j=1}^{n} \left(X_{a_j}^{high} - X_{a_j}^{low} \right)}{2^n} \tag{12}$$

After finding the trusted nodes, the data encrypted using AES [17] algorithm is forwarded through these trusted nodes.

V. Simulation Results

The performance of the proposed HCPT technique is analyzed by two different test scenarios and it is simulated using network simulator NS-2 tool. In the simulation run, we have used the parameter values as shown in Table 1. Consider a large number of nodes within 500 meter x 500 meter for different test scenarios. The transmission range of user is 250m. The sensing range of users is 30m , an initial energy of nodes is 100 joules, the initial power consumption of transmitting circuit is 15.9mW and the receiving circuit is 22.2mW. The testing scenario is varying the number of nodes between 50 to 250 with a fixed node speed. The proposed HCPT technique is compared with the existing state-of-art techniques such as DSR [18], 2-ACK scheme [14]. The performance is evaluated mainly, for the following metrics.

- Packet delivery ratio: The ratio of the number of packets received at the destination to the number of packets sent by the source.
- Routing overhead: The ratio of the amount of routing-related control packet transmissions to the amount of data transmissions
- Average end-to-end delay: The average time taken for a packet to be transmitted from the source to the destination.
- Throughput: The rate at which total amount of data is received at the destination. It is the number of bits transmitted per second ,ie, application traffic.

TABLE I. SIMULATION PARAMETERS

Simulation area	800 X 800 m^2
Number of nodes	50, 100, 150, 200, and 250
Node mobility	2, 4, 6, 8, 10 m/s
MAC	IEEE 802.11n physical
Transmission range of node	250 m
Sensing range of CS node	30 m
Initial energy of nodes	100 joules
Traffic type	CBR (TT-1 and TT-2)
Packet size	1024 bytes
Simulation Time	100 seconds

A. Impact of node density

The performance is analyzed by varying the number of node as 50, 100, 150, 200, and 250 with a fixed node speed say, 10 m/s. Fig. 2 shows the packet delivery ratio of proposed HCPT and existing DSR [18] and 2-ACK [14]. The plot clearly depicts that the packet delivery ratio of proposed HCPT technique is very high compared to the existing techniques. Fig.3 shows the routing overhead of proposed HCPT and existing DSR [18] and 2-ACK [14]. The plot clearly depicts that the routing overhead of proposed HCPT technique is very low compared to the existing techniques. Fig.4 shows the average end-to-end delay of proposed HCPT and existing DSR [18] and 2-ACK [14]. The plot clearly depicts that the average end-to-end delay of proposed HCPT technique is very low compared to the existing techniques. Fig.5 shows the throughput of proposed HCPT and existing DSR [18]

and 2-ACK [14]. The plot clearly depicts that the throughput of proposed HCPT technique is very high compared to the existing techniques.

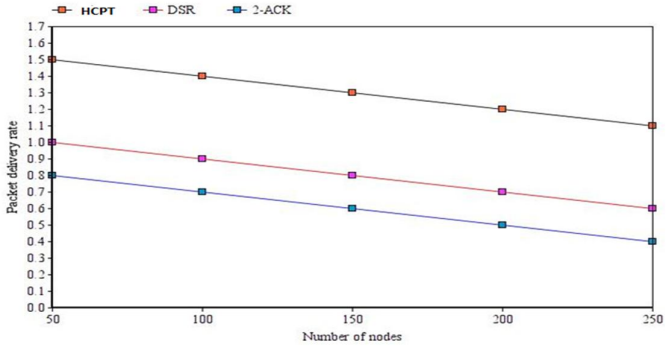

Figure 2. Packet delivery ratio with number of nodes

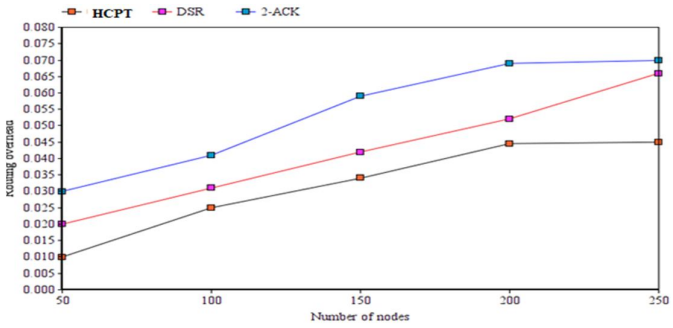

Figure 3. Routing overhead with number of nodes

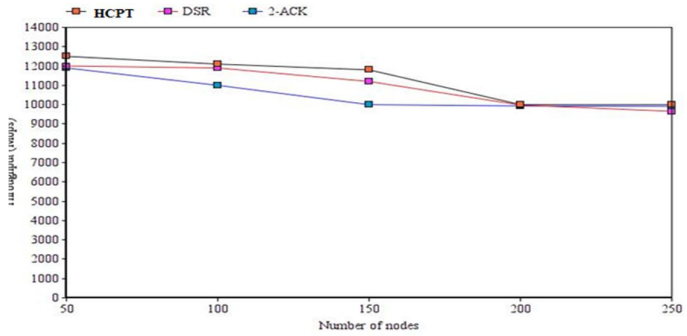

Figure. 4 Throughput with number of nodes

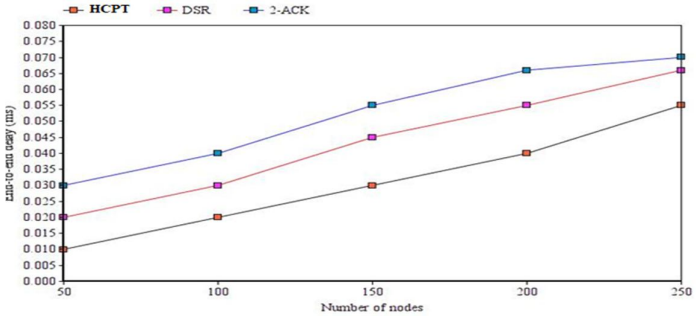

Figure. 5 Average end-to-end delay with number of nodes

VI. Conclusion

The proposed mechanism for detecting malicious nodes in MANETs under collaborative black hole attacks has proven efficient. Cryptographic technique such as AES algorithm used to encrypt the data and the Swarm based optimal trust inference model used to compute trust of each node were useful to compute forwarding node for data transferring purpose. The simulation results reveal that the proposed scheme outperforms the benchmark techniques such as DSR and 2ACK schemes, in terms of routing overhead, packet delivery ratio, throughput and delay.

References

[1] Sabato, C. Niezrecki and G. Fortino, "Wireless MEMS-Based Accelerometer Sensor Boards for Structural Vibration Monitoring: A Review", IEEE Sensors Journal, vol. 17, no. 2, pp. 226-235, 2017.

[2] Tamilarasan- Santhamurthy; "A Comparative Study of Multi-Hop wireless Ad-Hoc Network Routing Protocols in MANET ", IJCSI, International Journal of Computer Science Issues, Vol. 8,Issue 5, No 3, September 2011, PP:176-184.ISSN(online):1694-0814.

[3] Hilal Bello Said, Haider Kareem Abdulabbas, Mahmod Ismail:"Performance Evaluation of MANET Routing Protocols Based on Internet Protocols". International Journal of Engineering Research Volume No.4, Issue No.11, pp : 599-603, ISSN:2319-6890) 2347-5013, 01 Nov. 2015.

[4] Eric Astier, Abdelhakim Hafid and Sultan Aljahdal:" An efficient mesh-based multicast routing protocol in mobile ad hoc networks", WIRELESS COMMUNICATIONS AND MOBILE COMPUTING Wirel. Commun. Mob. Comput. (2010),Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/wcm.1016.

[5] J. Zhang, G. Song, G. Qiao, T. Meng and H. Sun, "An indoor security system with a jumping robot as the surveillance terminal", IEEE Transactions on Consumer Electronics, vol. 57, no. 4, pp. 1774-1781, 2011.

[6] S. Jokhio, I. Jokhio and A. Kemp, "Light-weight framework for security-sensitive wireless sensor networks applications", IET Wireless Sensor Systems, vol. 3, no. 4, pp. 298-306, 2013.

[7] A. Malatras, A. Asgari and T. Bauge, "Web Enabled Wireless Sensor Networks for Facilities Management", IEEE Systems Journal, vol. 2, no. 4, pp. 500-512, 2008.

[8] W. Wang, B. Bhargava, and M. Linderman, "Defending against collaborative packet drop attacks on MANETs," in Proc. 28th IEEE Int. Symp. Reliable Distrib. Syst., New Delhi, India, Sep. 2009.

[9] A.Rajaram, Dr. S. Palaniswami,"Malicious Node Detection System for Mobile Ad hoc Networks", International Journal of Computer Science and Information Technologies, Vol. 1 (2) , 2010.

[10] QualNet Simulaton Tool, Scalable Network Technologies. (Last retrieved March 18, 2013). [Online]. Available: http://www.qualnet.com

[11] P.-C. Tsou, J.-M. Chang, H.-C. Chao, and J.-L. Chen, "CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture," in Proc. 2nd Intl. Conf. Wireless Commun., VITAE, Chenai, India, Feb. 28–Mar., 03, 2011, pp. 1–5.

[12] A. Baadache and A. Belmehdi, "Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks," Intl. J. Comput. Sci. Inf. Security, vol. 7, no. 1, 2010.

[13] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proc. 6th Annu. Intl. Conf. MobiCom, 2000, pp. 255–265.

[14] K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[15] K. Vishnu and A. J Paul, "Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks," Int. J. Comput. Appl., vol. 1, no. 22, pp. 28–32, 2010.

[16] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc network," IEEE Commun. Mag., vol. 40, no. 10, Oct. 2002.

[17] M. Pitchaiah, Philemon Daniel, Praveen:"Implementation of Advanced Encryption Standard Algorithm", International Journal of Scientific & Engineering Research Volume 3,Issue 3,ISSN 2229-5518, March-2012.

[18] Shivashankar; H. N. Suresh; G. Varaprasad; G. Jayanthi "Designing Energy Routing Protocol With Power Consumption Optimization in MANET " IEEE Transactions on Emerging Topics in Computing Year: 2014, Volume: 2, Issue: 2 Pages: 192 - 97, DOI: 10.1109/TETC.2013.2287177.