ENERGY BASED ROUTING ALGORITHM FOR MOBILE AD HOC NETWORKS

[1]DR.A.RAJARAM, [2]S.KANNAN,
[1]Associate Professor, Department of Electronics and Communication Engineering,
Karpagam College of Engineering, Coimbatore, India.
[2]Research Scholar, Anna University, Chennai, India
E-mail: [1]gct143@gmail.com , [2]kannan340@gmail.com

ABSTRACT

An ad hoc network is an indivisible part of the networks. It is an infrastructureless network. Whenever node wants to communicate with neighborhood node, it does not depend on the centralized infrastructure. Ad hoc is dynamic in nature. Due to the open structure, node can be easily impersonated by the several attacks like Denial of Service (DoS) attack, Wormhole attack, black hole attack and Packet forwarding attack etc. In the presence of the attack, the energy consumption of the network can be increased unlimitedly. In this research work, we have considered three factors like node mobility, malicious behavior and unauthenticated node, in order to minimize the energy consumption of the node. By limiting these factors, the node consumes less energy. For that, we have developed the Energy Based Routing Algorithm (EBRA) which is integrated into the Dynamic Source Routing (DSR) protocol to ensure the minimum energy consumption rate. The proposed scheme consists of three phases. In first phase, nodes energy consumption is limited with the high mobility. In second phase, the effect of malicious behavior is reduced to avoid the replaying of packets. In third phase, the unauthenticated node is identified using the digital signature verification. By simulation results the proposed scheme achieves less energy consumption rate, more energy efficiency, better throughput, less overhead and delay in the presence of the malicious nodes than the existing schemes.

Keywords: *Ad Hoc Network, Dos Attack, Blackhole Attack, Wormhole Attack, Energy Efficiency , Energy Consumption Rate , Throughput, Delay And Overhead.*

1. INTRODUCTION

Wireless ad-hoc network is a decentralize type of wireless network. The network is ad hoc because it does not rely on a preexisting infrastructure or it does not have any access point. Instead, each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. In case of the classic routing, ad hoc networks can use flooding for forwarding the data [1]. An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to communicate with any other ad hoc network devices in link range. In recent years, ad hoc network refers to a mode of operation of IEEE 802.11 wireless networks.

Ad Hoc network is used for random and rapid deployment of a large number of nodes, which is a technology with a wide range of applications such as tactical communications, disaster relief operations, health care and temporary networking in areas that are not densely populated [2].Owing to the dynamic nature of Ad hoc networks, connections and position of all nodes are frequently changing. Therefore performance of network weakens rapidly. So, there is need for the development of a secure routing protocol [3, 4]. In Ad hoc network, we can classify the attacks in two types: (i) External attacks and (ii) Internal attacks. External attacks, in which the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services. Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviours [5]. From the literature survey, ad hoc routing is affected seriously in the presence of the malicious behaviour and has a harmful effect on network performance and reliability [6].

The rest of the paper is structured as follows. Section 2 gives an overview of Dynamic Source Routing (DSR) protocol. In Section 3, literature survey is presented. Section 4 presents the proposed Energy Based Routing Algorithm (EBRA). Section 5 illustrates the simulation results and analysis. Section 6 suggests methods used in real-life scenario. Section 7 describes the conclusion of the research work.

2. RELATED WORK

In the ad hoc networks presently in operation, the nodes are required to watch their neighbors for misbehaviour and this not only necessitates promiscuous modes of operation but also overloads the nodes. Marti et al. [8] proposed two approaches known as Watchdog and path rater approach In this approach, a node forwarding a packet checks if the next hop also forwards it. If not, a failure count is incremented and the upstream node is rated to be malicious if the count exceeds a certain threshold. The path rater module then utilizes this knowledge to avoid it in path selection. But this method is not suitable in case collision occurs.

Buchegger and Boudec [9] proposed a protocol called CONFIDANT, which aims at detecting and isolating misbehaving nodes, thus making misbehavior unattractive.Here misbehaving nodes are excluded from forwarding routes. This is method is lagging to detect the misbehaving nodes from good nodes.

Li Zhao et.al [10] have proposed MultipAth Routing Single path transmission (MARS) scheme to mitigate adverse effects of misbehavior. This scheme combines multipath routing and single path data transmission with end-to-end feedback mechanism to provide more comprehensive protection against misbehavior from individual or cooperating misbehaving nodes.

S.Umang et al. [11] presented the approach called Enhanced Intrusion Detection System (EIDS) for detecting malicious node and minimizing the energy consumption of the node in MANET. But this method does imply about the digital signature verification, node authentication.

Raza and Hussain [12] have introduced a specific node known as guard node. This scheme is based on trust calculation process in which if node has trust level lower than a pre-defined threshold, then it is identified as malicious. Moreover, this particular node will not be considered for route selection.

In [13], Mehfuz and Doja introduced a new secure power aware ant colony algorithm for detection of compromised and malicious nodes in MANETs.

Patwardhan et al. [14] have proposed an approach to secure a MANET using a threshold-based intrusion detection system and a secure routing protocol. Madhavi and Tai Hoon Kim [15] have proposed a MIDS (Mobile Intrusion Detection System) suitable for multi-hop ad-hoc wireless networks, which has detected nodes misbehavior, anomalies in packet forwarding, such as intermediate nodes dropping or delaying packets.

Syed Rehan Afzal et al. [16] have explored that the security problems and attacks in existing routing protocols and then they have presented the design and analysis of a secure on-demand routing protocol, called RSRP which confiscated the problems mentioned in the existing protocols. In addition, RSRP has used a very efficient broadcast authentication mechanism which does not require any clock synchronization and facilitates instant authentication

Muhammad Mahmudul Islam et al. [17] have presented a possible framework of a link level security protocol (LLSP) to be deployed in a Suburban Ad-hoc Network (SAHN). Their initial work has indicated that LLSP is a suitable link-level security service for an ad-hoc network similar to a SAHN.

Shiqun Li et al. [18] have explored that the security issues of wireless sensor networks, and in particular propose an efficient link layer security scheme. To minimize computation and communication overheads of the scheme, they have designed a lightweight CBC-X mode Encryption/Decryption algorithm that attained encryption/decryption and authentication all in one. As a result, security operations incur no extra byte in their scheme.

Jinhua Zhu and Xin Wang [19] developed the protocol to reduce the energy consumption while taking care of overhead and mobility. They proposed a PEER protocol with a quick and low overhead path discovery scheme and an efficient path maintenance scheme for reducing energy consumption especially in mobile environment. But this model does not suitable incase high overhead occurs.

Our aim in this paper is to arrive at a simple protocol which strikes a balance between defending against Malicious Nodes and energy consumption.

3. OVERVIEW OF THE PROPOSED SCHEME

Proposed work introduces a solution Energy Based Routing Algorithm (EBRA) to reduce the energy consumption of the node. The energy consumption is considered based on limiting the three factors like mobility, malicious behavior and unauthenticated node. In ad hoc networks, node can move in a arbitrary manner. It does not rely on any infrastructure. While increasing the movement of the node, the node mobility increases which leads to higher energy consumption. For that we have set one common threshold mobility factor (T_{mb}). This threshold makes some balances on energy consumption. Due to the presence of malicious behavior, the node replays more packets incase if the network connectivity is not available. So, more energy consumption is induced. Here, we have set the trust threshold vector (T_{tv}) to identify the malicious node which makes more consumption. All the nodes are communicating through the reliable route. Authenticated node is determined using digital signature (DS_{min}) by destination node. Based on these three factors, we have set common energy conservation rate. This rate determined whether the whole network consumes more energy or not. In the proposed algorithm, these three factors are being limited to minimize the energy consumption.

Step i) Limiting the Trust mobility factor (T_{mb})

Once the route discovery process is initiated, the source node keeps updating the routing table of all nodes. Here each node having its own energy power. Let us define the range R, the node i move with high mobility in the region. Due to the randomness of node locations, this speed may be faster or slower when the packet travels through different subareas in the network. The trust mobility factor is based on the information speed ϖ_{ψ}(t) and the long term speed $\omega\ \phi$.

To evaluate the actual information speed ϖ_{ψ}(t), without considering the subarea bias,

$$\varpi_{\psi}(t) = \frac{|\lambda_{\psi}(t)|}{t} \qquad (1)$$

$\lambda_{\psi}(t)$ is the line segment where the information is propagated in wireless ad hoc networks. Here the packet is transmitted for t seconds.

The Long term speed in the direction ϕ is given as

$$\omega\ \phi = \lim_{t\to\infty} \left(\frac{\vartheta}{t}\right)^{\gamma} \qquad (2)$$

ϑ is a direction where the information is propagated through a particular path as a function of time.

The trust mobility factor is derived as combination of both actual information speed and long term speed.

$$T_{mb} = \varpi_{\psi}(t) + \omega\ \phi - \mathrm{DCT}\ (\varpi_{\psi}(t)\ , \omega\ \phi) \qquad (3)$$

We used Discrete Cosine Transform (DCT) for reducing energy consumption of the node. By constantly keeping trust mobility factor within the given the region R, node consumes less energy.

Step ii) Keeping minimal energy consumption in the presence of the malicious node.

In our work, we consider three factors like node proposal, node familiarity and node awareness to identify the malicious node. The trust threshold vector is set based on these three factors.

Nodes proposal is also used to identify the malicious behaviors. Evaluating the proposals is given by NP_Q^P which is node P's evaluation to node Q by collecting recommendations,

Node proposal is derived as,

$$NP_Q^P = \frac{\sum_{\upsilon\in\gamma} V\,|\,P\to Q\,|\,{*}V\,|\,R\to Q\,|}{V\,|\,P\to R\,|} \qquad (4)$$

γ is a group of recommenders.

$V\,|\,P\to R\,|$ is trust vector of node P to R.

$V\,|\,R\to Q\,|$ is trust vector of node R to Q.

Node familiarity NF_Q^P is given as,

$$\frac{Outcoming\ packets\ from\ node\ Q - Packets\ from\ node\ Q\ to\ P}{Incoming\ packets\ from\ node\ Q\ - Packets\ from\ node\ P\ to\ Q} \qquad (5)$$

Nodes awareness NA_Q^Pcan be defined by,

NA_Q^P= (1-$p_{P,Q}$) * (1-$p_{Q,P}$) (6)

Probability can be defined by NA_Q^P which is node P's evaluation to node Q by directly determining MAC layer link quality between node P and node Q on the physical layer. $P_{P,Q}$ is packet loss probability from node P to node Q, while , $p_{Q,P}$ is packet loss probability from node Q to node P.

The Trust threshold vector T_{tv} is derived as the combination of above three factors,

$$T_{tv} = NP_Q^P + NF_Q^P + NA_Q^P \quad (7)$$

Incase if any node below the T_{tv} , the node is considered as malicious node. Once the malicious node is identified, it is isolated from the network. Then we find the shortest path to the desired destination node for routing the packets. By doing this, the replaying of packets will be reduced. So the energy consumption of the node can be reduced.

Step iii) Detection of misbehaving node by means of digital signature verification.

Let {T_{v1}, T_{v2}…} be the initial trust vectors of the nodes {n_1, n_2…} along the route R1 from a source S to the destination D.

Since the node does not have any information about the reliability of its neighbors in the beginning, nodes can neither be fully trusted nor be fully distrusted. When a source S want to establish a route to the destination D, it send route request (RREQ) packets.

When the destination D receives the accumulated RREQ message, it measures the number of packets received P_{rec}.

Then it constructs a route on Prec with the key shared by the sender and the destination. The RREP contains the source and destination ids, the route of P_{rec}, the accumulated route from the RREQ, which are digitally signed by the destination. The RREP is sent towards the source on the reverse route R1. The intermediate node then verifies the digital signature of the destination node stored in the RREP packet, is valid. If the verification fails, then the RREP packet is dropped. Otherwise, it is signed by the intermediate node and forwarded to the next node in the reverse route.

When the source S receives the RREP packet, if first verifies that the first id of the route stored by the RREP is its neighbor. If it is true, then it verifies all the digital signatures of the intermediate nodes, in the RREP packet. The digital signature includes recommendation about the neighbor node and probability that data packet received successfully. If all these verifications are successful, then the trust counter values of the nodes are incremented as

$$Tv_i = Tv_i + \alpha_1 \quad (8)$$

If the verification is failed, then

$$Tv_i = Tv_i - \alpha_1 \quad (9)$$

Where α_1 is the step value, which can be assigned a small fractional value during simulations. After this verification stage, the source S check the digital signature values DS of the nodes n_i.

For any node n_k, if $DS_k < DS_{min}$, where DS_{min} is the minimum threshold value, its trust vector value is further decremented as

$$Tv_i = Tv_i – \alpha_2 \quad (10)$$

For all the other nodes with $DS_k > DS_{min}$, the trust counter values are further incremented as

$$Tv_i = Tv_i + \alpha_2 \quad (11)$$

Where α_2 is another step value with $\alpha_2 < \alpha_1$.

When $DS_k < DS_{min}$, the node is considered as a unauthenticated node. If the source does not get the RREP packet or RERR packet for a time period of t seconds, it will be considered as a node failure or link failure. Then the route discovery process is initiated by the source again. Once the unauthenticated node has been detected by source node, it will be isolated. Here we are providing authentication to all the nodes.

4. PERFORMANCE EVALUATION

The performance of the proposed approach is evaluated in this section. The simulation model is discussed in Section 6.1 and the simulated results are presented and described in Section 6.2.

4.1 Simulation Model and Parameters

We assess the proposed algorithm for malicious node detection in MANETs and compare it with the existing routing protocol DSR in MANET using simulations. We have simulated our results using ns2.34 [20] simulator. Here we made the assumption that adopted for simulation is all nodes are moving dynamically including the direction and speed of nodes. Moreover, Brijesh et al. [21] have used stationary nodes for malicious node detection and have not focused on direction and speed of nodes in their approach. Therefore this scheme is not applicable in random scenario. Taking this point of view, our solution is a better approach than [21].

Mobility scenario is generated by using random way point model with 300 nodes in an area of 1000 m × 1000 m. The simulation parameters are mentioned below in Table 1

Our simulation settings and parameters are summarized in table 1

No. of Nodes	300
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point
Initial energy	75
Transmitted power	0.879
Received Power	0.08
Pause time	150 s
CS range	540m

B. Performance Metrics

We evaluate mainly the performance according to the following metrics.

Average Packet Delivery Ratio: It is the ratio of the number of packets received successfully and the total number of packets transmitted.

Routing Overhead: The control overhead is defined as the total number of routing control packets normalized by the total number of received data packets.

In end-to-end delay, a packet depends on the routing discovery latency, additional delays at each hop and number of hops.

C. Results

The results are examined by using performance metrics end-to-end delay, packet delivery percentage and energy consumption. We increase percentage of malicious nodes and total number of nodes presented. For 300 nodes, we vary the presence of 0 malicious nodes to 95. We repeat the experiments by increasing total number of nodes present in the network.

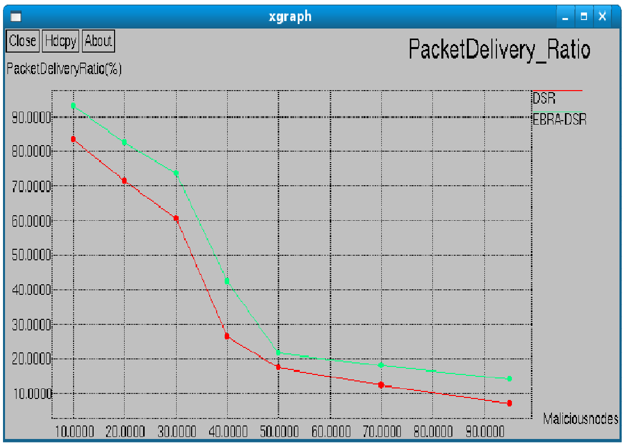

Fig 1. Packet Delivery Ratio

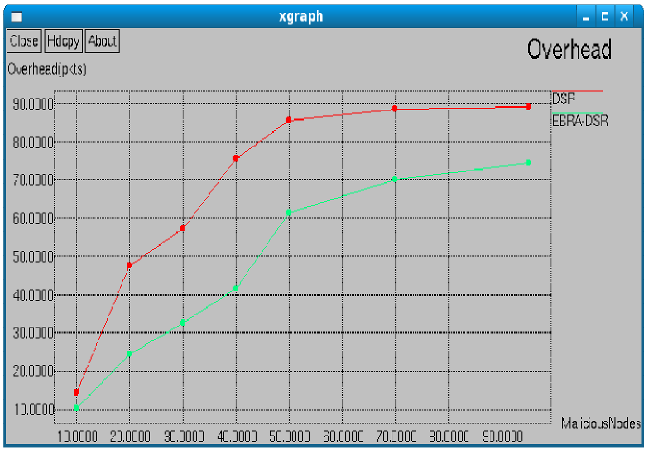

Fig 2. Relative Overhead

In Fig1 & 2, we vary the malicious nodes from 0 to 95. While increasing the number of malicious nodes the packet delivery ratio of proposed algorithm EBRA-DSR achieves better than the DSR. In Fig 3, the EBRA-DSR achieves less overhead than DSR. Generally DSR has higher overhead. But our proposed scheme achieves less overhead.

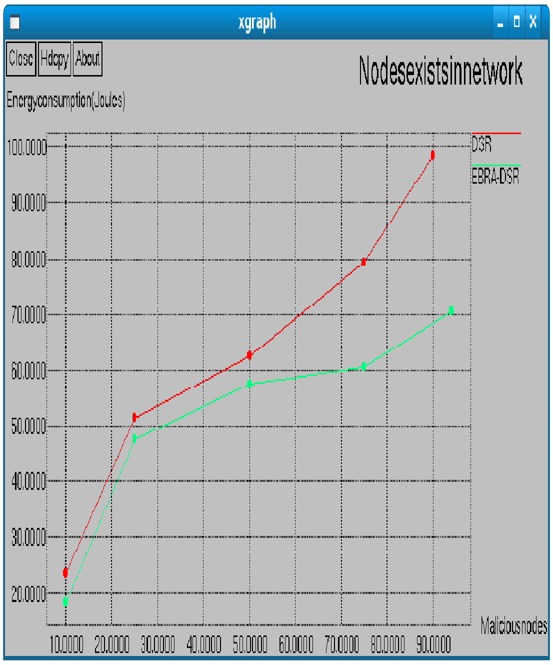

Fig 3. Energy Consumption Vs Malicious Nodes

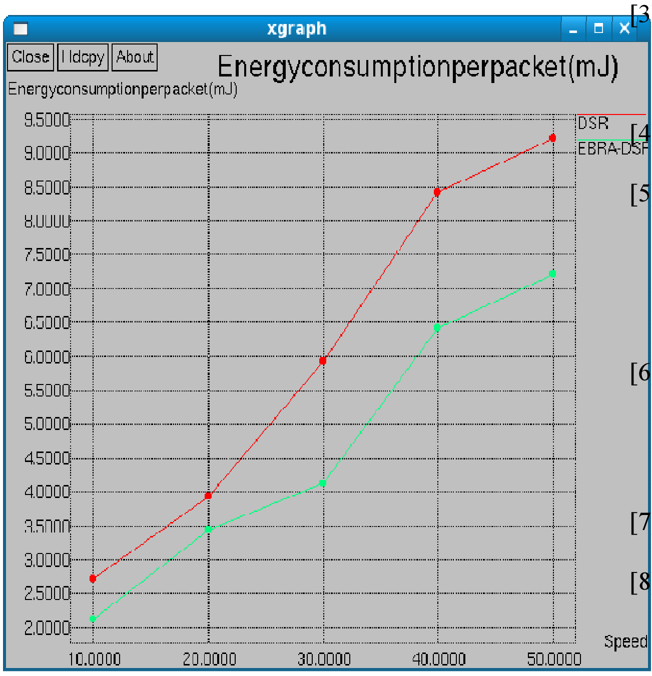

Fig 4. Energy Consumption Vs Speed

In Fig 3, we vary the malicious nodes from 0 to 95. The energy consumption of EBRA-DSR achieves low than the DSR. In Fig 4, speed is varied as 10,20….50. When we increase the speed, the mobility is also get increasing. The proposed algorithm EBRA-DSR has low energy consumption per packet than the existing routing protocol DSR.

5. CONCLUSION

In this research work, an energy based routing algorithm is proposed for energy consumption in ad hoc networks. The proposed algorithm is implemented using Dynamic Source Routing (DSR) Protocol. By simulation results, the EBRA-DSR is better than DSR in the presence of malicious nodes. The proposed work can be a suggestive approach for a real life approach such as military and defense. Future studies can be extended to implement the EBRA – DSR for other routing protocols like DSDV, ZRP by considering a lot of energy consumption, high overhead and energy cost.

REFERENCES:

[1] C K Toh, Ad Hoc Mobile Wireless Networks, Prentice Hall Publishers , 2002

[2] Sanjay K. Dhurandher, Mohammad S et.al , “FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems”, *IEEE Systems Journal*, Vol. 5, No. 2, June 2011.

[3] Perkins C.E., Royer E.M.: ‘Ad hoc on demand distance vector (AODV) routing’. Internet draft, draft-ietf-manetaodv- 02.txt, November 1998

[4] Siva C., Murty R., Manoj B.S.: ‘Ad hoc wireless networks’ (Pearson, 2005)

[5] Pradip M. Jawandhiya, Mangesh M. Ghonge & Dr. M.S.Ali , “A Survey of Mobile Ad Hoc Network Attacks”, *International Journal of Engineering Science and Technology,* Vol. 2(9), 2010, 4063-4071.

[6] YAU P.-W., MITCHELL C.-J.: ‘Reputation methods for routing security for mobile ad hoc networks’. 2003, doi: 10.1.1.3.7733,*http://www.isg.rhul.ac.uk/_cjm/rmfrsf.pdf*

[7] “Dynamic Source Routing ” From *Wikipedia, the free encyclopedia.*

[8] S.Marti,T.J.Giulli,K.Lai and M.Baker , “Mitigating routing misbehavior in mobile adhoc network”, *Mobile computing and networking*,2000,pp. 255- 265

[9] S. Buchegger and J. Boudec, “Performance Analysis of the Confidant Protocol,” *Proc. Int’l Symp, Mobile Ad Hoc Networking and Computing*, 2002.

[10] Zheng Yan and peng Zhang, “Trust Evalution based security solution in Adhoc network”, pp 1- 14.

[11] S. Umang, B.V.R. Reddy& M.N. Hoda , “Enhanced intrusion detection system for malicious node detection in ad hoc routing protocols using minimal energy consumption”, *IET Commun.,* 2010, Vol. 4, Iss. 17, pp. 2084–2094.

[12] Raza I., Hussain S.A.: ‘Identification of malicious nodes in an AODV pure ad hoc network through guard nodes’, *ACM Comput. Commun*., 2008, 31, (9), pp. 1796–1802.

[13] Mehfuz S., Doja M.N.: ‘Swarm intelligent power-aware detection of unauthorized and compromised nodes in MANETs’, J. *Artif. Evol. Appl*., 2008, 2008, article id 236803. p. 16. doi:10.1155/2008/236803.

[14] A.Patwardhan, J.Parker, M.Iorga, A. Joshi, T.Karygiannis and Y.Yesha “Threshold-based Intrusion Detection in Adhoc Networks and Secure AODV” Elsevier Science Publishers B. V., *Ad Hoc Networks Journal* (ADHOCNET), June 2008.

[15] S.Madhavi and Dr. Tai Hoon Kim “An Intrusion Detection System In Mobile Adhoc networks” *International Journal of Security and Its Applications*, Vol. 2, No.3, July, 2008.

[16] Afzal, Biswas, Jong-bin Koh,Raza, Gunhee Lee and Dong-kyoo Kim, "RSRP: A Robust Secure Routing Protocol for Mobile Ad Hoc Networks", in *proceedings of IEEE Conference on Wireless Communications and Networking,* pp.2313-2318,April 2008.

[17] Muhammad Mahmudul Islam, Ronald Pose and Carlo Kopp, "A Link Layer Security Protocol for Suburban Ad-Hoc Networks", *in proceedings of Australian Telecommunication Networks and Applications Conference*, December 2004.

[18] Shiqun Li, Tieyan Li, Xinkai Wang, Jianying Zhou and Kefei Chen, "Efficient Link Layer Security Scheme for Wireless Sensor Networks", *Journal of Information And Computational Science*, Vol.4, No.2,pp. 553-567, June 2007.

[19] Jinhua Zhu and Xin Wang, “Model and Protocol for Energy-Efficient Routing over Mobile Ad Hoc Networks”, *IEEE Transactions on Mobile Computing*, Vol. 10, No. 11, November 2011, pp.1546-1557.

[20] *ww.isi.edu/nsnam, ns2 manual*

[21] Brijesh P.A., Yadav S., Chandra J.: ‘Statistical analysis based efficient decentralized intrusion detection scheme for mobile ad hoc networks’. 2008, doi: 10.1109/ ICON.2008.4772601.