Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 10 Version 1.0 May 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Energy Efficient, Secure and Stable Routing Protocol for MANET

By Sunil Taneja & Ashwani Kush

Aruna Asaf Ali Government Post Graduate College, Haryana, India

Abstract - Mobile Adhoc Network (MANET) is characterized by mobile hosts, dynamic topology, multi-hop wireless connectivity and infrastructureless ad hoc environment. The adhoc environment is accessible to both legitimate network users and malicious attackers. Moreover, as the wireless links are highly error prone and can go down frequently due to mobility of nodes, therefore, energy efficient, secure and stable routing over MANET is still a very critical task due to highly dynamic environment. In this research paper, an effort has been done to combine these factors of security, power and stable routing by proposing a new protocol EESSRP (Energy Efficient, Secure and Stable Routing Protocol). An experimental analysis of proposed protocol has been carried out using network simulator NS-2.34. An effort has been made to perform analysis using random way point mobility model. The results have been derived using self created network scenarios for varying number of mobile nodes. The performance metrics used for evaluation are packet delivery ratio, average end to end delay, throughput, normalized routing load and packet loss. It has been concluded that the proposed protocol i.e. EESSRP provides energy efficient, secure and stable routing strategy for mobile adhoc networks.

Keywords : *EESSRP, Energy Efficient, MANET, Protocol, Routing, Secure, Stable.*

GJCST-E Classification: *C.2.1*

Strictly as per the compliance and regulations of:

Energy Efficient, Secure and Stable Routing Protocol for MANET

Sunil Taneja [α] & Ashwani Kush [σ]

Abstract - Mobile Adhoc Network (MANET) is characterized by mobile hosts, dynamic topology, multi-hop wireless connectivity and infrastructureless ad hoc environment. The adhoc environment is accessible to both legitimate network users and malicious attackers. Moreover, as the wireless links are highly error prone and can go down frequently due to mobility of nodes, therefore, energy efficient, secure and stable routing over MANET is still a very critical task due to highly dynamic environment. In this research paper, an effort has been done to combine these factors of security, power and stable routing by proposing a new protocol EESSRP (Energy Efficient, Secure and Stable Routing Protocol). An experimental analysis of proposed protocol has been carried out using network simulator NS-2.34. An effort has been made to perform analysis using random way point mobility model. The results have been derived using self created network scenarios for varying number of mobile nodes. The performance metrics used for evaluation are packet delivery ratio, average end to end delay, throughput, normalized routing load and packet loss. It has been concluded that the proposed protocol i.e. EESSRP provides energy efficient, secure and stable routing strategy for mobile adhoc networks.

Keywords : EESSRP, Energy Efficient, MANET, Protocol, Routing, Secure, Stable.

I. Introduction

MANET is self-organizing, rapidly deployable, and requires no fixed infrastructure. An Adhoc wireless network is a collection of mobile devices equipped with interfaces and networking capability. It is adaptive in nature and is self organizing. A formed network can be de-formed and again formed on the fly and this can be done without the help of system administration. Each node may be capable of acting as a router. Applications include but are not limited to virtual classrooms, military communications, emergency search and rescue operations, data acquisition in hostile environments, communications set up in exhibitions, conferences and meetings, in battle field among soldiers to coordinate defence or attack, at airport terminals for workers to share files etc. Although security has long been an active research topic in wired networks, the unique characteristics of Adhoc networks present a new set of nontrivial challenges to security design. These challenges include open network architecture, shared wireless medium, stringent resource constraints, and highly dynamic topology. Consequently, the existing security solutions for wired networks do not directly apply to the Adhoc environment. The main goal of the security solutions for an Adhoc network is to provide security services, such as authentication, confidentiality, integrity, anonymity and availability to mobile users [2]. One distinguishing characteristic of this network from the security design perspective is the lack of a clear line of defense. Unlike wired networks that have dedicated routers, each mobile node in an adhoc network may function as a router and forward packets for other peer nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. In such an environment, there is no guarantee that a path between two nodes would be free of malicious nodes, which would not comply with the employed protocol and attempt to harm the network operation. Another major hurdle in communication via Adhoc networks is their power limitations. As most of them use battery power and also are moving so there is always limitation of battery power. A new scheme has been proposed here to incorporate security and power features in adhoc networks. The scheme takes care of basic security needs and uses concept of Hash Key generation to attain the goal of security. It uses route table entry for its power status. The work is an extension of earlier work done [3, 4] in the fields of power, security and stability. The scheme has been incorporated on the refined version of SSRP (Stable and Secure Routing Protocol) [3] and AODV (Adhoc On-Demand Distance Vector Routing Protocol) [5].

II. Energy Efficient and Stable Routing

An ad hoc network consists of hosts communicating among themselves with portable radios. This network can be deployed without any wired base station or infrastructure support where routes are mainly multi-hop because of the limited radio propagation range. The nodes in an ad hoc network are constrained by battery power for their operation. To route a packet from a source to a destination involves a sufficient number of intermediate nodes. Battery power of a node is a precious resource that must be used efficiently in order to avoid early termination of a node or a network. One distinguishing feature of Energy Efficient ad hoc

Author α : Department of Computer Science, Smt. Aruna Asaf Ali Government Post Graduate College, Kalka-133 302, Haryana, India.
E-mail : suniltaneja.iitd@gmail.com
Author σ : Department of Computer Science, University College, Kurukshetra University, Kurukshetra-132 119, Haryana, India.
E-mail : akush20@gmail.com

routing protocol is its use of Power for each route entry. Given the choice between two routes to a destination, a requesting node is required to select one with better power status and more active.

Efficient battery management [6, 7, 8], transmission power management [9, 10] and system power management [11, 12] are the major means of increasing the life of a node. These management schemes deal in the management of energy resources by controlling the early depletion of the battery, adjust the transmission power to decide the proper power level of a node and incorporate low power consumption strategies into the protocols. Typical metrics used to evaluate ad hoc routing protocols are shortest hop, shortest delay and locality stability. However, these metrics may have a negative effect in MANETs because they result in the over use of energy resources of a small set of nodes, decreasing nodes and network lifetime. The energy efficiency of a node is defined by the number of packets delivered by a node in a certain amount of energy.

A few reasons for energy management in MANETs are:

a) Ad hoc networks have been developed to provide communication for an environment where fixed infrastructure cannot be deployed. Nodes in ad hoc networks have very limited energy resources as they are battery powered.
b) In so many situations like hostile territory, it is very difficult or almost impossible to replace the battery or recharge it.
c) There is no central coordinator in case of ad hoc networks as a base station in cellular networks.

Therefore ad hoc networks work on the concept of multi-hop routing in which intermediate nodes play the role of the relay nodes. If the relay traffic is very high, it leads to rapid depletion of a node and if the traffic is negligible upon a node that leads to the partitioning of a network. If the battery size is very small, it decreases the lifetime of a node and if battery size of a node is large, it increases the weight of the mobile node. So to keep the standard small size of a battery, energy management techniques are required to utilize it efficiently. Optimal value selection for transmitting a packet is difficult but as this transmission power increases, it increases the consumption of the battery but the connectivity increases. This increases the number of paths to the destination. Therefore selection of the transmission power should be done in order to reduce the consumption of the battery power so as to maximize the simultaneous packet transmission and preserve connectivity.

Energy control algorithms [13, 14, 15] are very useful for the systems in which the available bandwidth is shared among all the users. Reduction in transmission power increases frequency reuse, which leads to better channel reuse. Although developing battery efficient systems that have low cost and complexity, remains a crucial issue. Efficient battery aware protocol is the need of today's ad hoc networks. Designing smart battery packs that can select appropriate battery discharge policies under different load conditions is a challenging problem. Other issues that exist at the physical layer includes efficient battery scheduling techniques[15] selection of an optimal transmission power for the nodes and finding the appropriate time duration for switching off the nodes . Investigations at data link layer are; addressing the issues of relay traffic, such as finding an optimal strategy that decides the amount of allowable relay traffic for a node. Developing battery aware MAC algorithms for the nodes that increase the lifetime of the nodes is an important issue. Finally, at the network layer designing of an efficient routing algorithm that increases the network lifetime by selecting an optimal relay node.

The network layer can aid in the conservation of energy by reducing the power consumed for two main operations, namely, communication and computation. The communication power consumption is mainly due to transmission and reception of bits. Whenever a node remains active, it consumes power. Even when the node is not actively participating in communication, but is in the listening mode waiting for the packets, the battery keeps discharging. The computation power consumption refers to the power spent in calculations that take place in the nodes for routing and other decisions. The following section discusses some of the power-efficient routing algorithms. In general, a routing protocol which does not require large tables to be downloaded or greater number of calculations is preferable, the amount of data compression before transmission decreases the power consumed for communication although the number of computation tasks increases. Since the energy required per bit for communication is hundred times compared to computation, data compressed is preferred. MANETs allow anywhere, any time network connectivity with complete lack of control, ownership and regulatory influence. Each node in a MANET participates in the routing function. To establish communication among different nodes, the "death" of few nodes is possible due to energy exhaustion.

In traditional routing algorithms, routes are constructed on the basis of shortest path but these protocols are not aware of the energy consumed for the path setup or maintenance. Shortest path algorithm may result in a quick depletion of the energy of nodes along the heavily used routes.

Designing energy aware routing protocols has attracted a lot of attention for prolonged network operational time. Design objective of energy aware protocols is to select energy efficient routes and simultaneously minimizing the overhead incurred in the selection of the routes. Some routing algorithms given

by [16, 17] can optimize the energy use with a global perspective. But these algorithms incur expensive overheads for gathering, exchanging and storing the state information. These algorithms can be improvised in order to make them scalable. For this purpose a localized topology controlling algorithm [16] or a distributed energy aware dominating set generating algorithm [18] can be applied on nodes and a traditional base algorithm like AODV or DSR may be run in the network. This kind of protocol design can reduce the communication overheads consumed for route discovery. Implementation of this kind of approach requires the knowledge of one or two hop neighbours at the nodes. This requirement can consume bandwidth and use energy for gathering such information at nodes constantly in dynamic networks. Some algorithms [16, 19, 20] work without assuming any topological knowledge at nodes and they can avoid the proactive overheads required for topological information. These kind of on demand approaches are required for energy efficient paths. Due to the reactive nature of on demand protocols, these are more energy efficient in MANETs and therefore in this chapter, only on demand protocols have been analyzed on the anvil of their energy, so that selection of a better base protocol may lead to find energy efficient paths. A lot of work has been carried in the direction of energy aware routing. They modify either AODV or DSR, which are taken as the base protocol. An Energy and Delay Constrained Routing in MANETs have been proposed by Laura et al. [21], in which energy saving and timely delivery of data packets is incorporated into the route discovery phase to select paths with lower cost. This algorithm utilizes two metrics, residual energy and queue length at each node. Buffer information is considered as a traffic load characteristic and its use is to limit the battery power consumption and end to end delay. Chen et al. [22] have proposed an Energy Efficient AODV for Low Mobility Ad hoc Networks, in which the node energy consumption of the overall network is reduced by dynamically controlling the transmission power by utilizing a novel route cost metric. Three extensions to the traditional AODV protocol, named Local Energy Aware Routing (LEAR-AODV), Power Aware Routing (PAR-AODV) and Lifetime Prediction Routing (LPR-AODV) have been proposed by [23], for balanced energy consumption in MANETs. These algorithms use energy consumption as a routing metric and try to reduce the nodes energy consumption by routing packets using energy optimal routes. Li et al. [16] have proposed an algorithm to maximize the network life time by balancing the energy draining rates among nodes using precise global state information. Narayanaswami et al. [24] have designed an approach named COMPOW, which works to find the minimal common value of node transmission range to maintain the network connectivity. COMPOW attempts to satisfy three major objectives. Increasing the battery lifetime of all the nodes, increasing the traffic carrying capacity of the network and reducing the contention among the nodes. The main reason behind the need for an optimal transmit power level for the nodes in MANETs is that battery power is saved by reducing the transmission range of the node. It has been proved by Kawadia et al. [36] that the COMPOW protocol works only in a network with a homogeneous distribution of nodes. CLUSTERPOW is an extension of COMPOW for non-homogeneous dispersion of the nodes. It is a power control clustering protocol in which each node runs a distributed algorithm to choose the minimum power p to reach the destination through multiple hops. Unlike COMPOW, where all the nodes of the network agree on a common power level, in CLUSTERPOW the value of p can be different for different nodes and is proved to be in non-increasing sequence toward the destination. An extended approach to COMPOW is used to reduce the energy consumed in packet forwarding for heterogeneous networks. These approaches introduce the excessive overheads and they have the scalability issue. Some pure on demand energy aware approaches have also been designed. Xue et al. [25] have introduced a location aided routing with energy awareness. In this approach each node with a packet to forward performs per hop power aware forwarding with the help of location information of the destination, neighbouring nodes and the node itself. With this approach good energy efficiency can be achieved but at the cost of more resource consumption for updating and collecting the information in the dynamic environment of MANETs.

III. Secure Routing

Security is an important issue for ad hoc networks, especially for those security-sensitive applications. It has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. The salient features of ad hoc networks pose both challenges and opportunities in achieving the aforementioned goals. *First,* use of wireless links renders an ad hoc network susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay, and message distortion. Eavesdropping might give an adversary access to secret information, violating confidentiality. Active attacks might allow the adversary to delete messages, to inject erroneous messages, to modify messages, and to impersonate a node, thus violating availability, integrity, authentication, and non-repudiation. *Secondly*, nodes, roaming in a hostile environment e.g. in a battlefield with relatively poor physical protection, have non-negligible probability of being compromised. Therefore, one should not only consider malicious attacks from outside a network, but also take into account the attacks launched from within

the network by compromised nodes. Therefore, to achieve high survivability, ad hoc networks should have a distributed architecture with no central entities. Introducing any central entity into our security solution could lead to significant vulnerability; that is, if this centralized entity is compromised, then the entire network is subverted. *Thirdly,* an ad hoc network is dynamic because of frequent changes in both its topology and its membership. Trust relationship among nodes also changes, for example, when certain nodes are detected as being compromised. Unlike other wireless mobile networks, such as mobile IP, nodes in an ad hoc network may dynamically become affiliated with administrative domains. Any security solution with a static configuration would not suffice. It is desirable for our security mechanisms to adapt on-the-fly to these changes. *Finally,* an ad hoc network may consist of hundreds or even thousands of nodes. Security mechanisms should be scalable to handle such a large network.

These challenges motivate for building multi fence security solutions that achieve both broad protection and desirable network performance. Basically, the complete security solution should span both layers, and encompass all three security components of prevention, detection, and reaction. The dilemma is that how should it be judged whether the mobile ad hoc network is secure or not. Some of the main security attributes [26, 27] that are used to inspect the security state of the mobile ad hoc networks are availability, integrity, confidentiality, authenticity, non repudiation, authorization and anonymity.

In mobile ad hoc networks, radio transmission is the most common means of communication. Eavesdropping on a node is far easier than in wired networks. Since intermediate nodes no longer belong to a trusted infrastructure, but may be eavesdroppers as well, consequent end-to-end encryption is mandatory. Next, as all nodes in an Ad hoc network cooperate in order to discover the network topology and forward packets, denial of service attacks on the routing function are very easy to mount. Nodes may create stale or wrong routes, creating black holes or routing loops. Furthermore, in ad hoc networks exists a strong motivation for non-participation in the routing system. Both the routing system and the forwarding of foreign packets consume a node's battery power, CPU time, and bandwidth, which are restricted in mobile devices. Consequently, selfish nodes may want to save their resources for own use. There are three main causes for a node not to work according to the common routing protocol. Malfunctioning nodes are simply suffering from a hardware failure or a programming error. Although this is not an attack, they may cause severe irritation in the routing system of an ad hoc network. Selfish nodes try to save their own resources, as described above. Malicious nodes are trying to sabotage other nodes or even the whole network, or compromise security in some way. Before developing a security framework that prevents selfish or malicious nodes from harming the network, it is worthwhile to first create a structured overview on what kinds of attacks are possible in ad hoc networks. Network security attacks [25, 26] are typically divided into two categories passive vs. active attacks which have already been discussed in previous chapter. MANETs are extremely vulnerable to attacks due to their dynamically changing topology, absence of conventional security infrastructures and open medium of communication, which, unlike their wired counterparts, cannot be secured with ease. MANET security involves authentication, key establishment and distribution, and encryption. Despite the fact that security of ad hoc routing protocols is causing a major roadblock in commercial applications of this technology, only a limited work has been done in this area. Such efforts have mostly concentrated on the aspect of data forwarding, disregarding the aspect of topology discovery. On the other hand, solutions that target route discovery have been based on approaches for fixed-infrastructure networks, defying the particular ad hoc network challenges. To address these concerns, several secure routing protocols have been studied and some of the popular secured protocols are ARAN [28], SEAD [29], SRP [30], SECURE AODV [31], SLSP [32], ARIADNE [33] and SAR [34].

IV. Proposed Algorithm

The proposed algorithm takes care of three core issues of energy efficient, secure and stable routing over mobile ad hoc networks is given below:

a) Secure Routing

In the proposed algorithm, secure routing has been implemented in three steps:

(i) Diffie-Hellman Algorithm of key exchange for generation of secret key
(ii) Apply hashing to generate subsequent keys over selected route
(iii) Encryption and Decryption using XOR operation

b) Energy Efficient and Stable Routing

In the proposed algorithm, energy efficient and stable routing has been implemented in five steps:

(i) The source node S broadcasts RREQ message containing threshold value Th.
(ii) At a neighbor node N, If En > ETh a reply message is sent otherwise no reply is sent
(iii) At the source node S, all reply messages are scanned. The neighbour with shortest active route is selected for forwarding the data and other nodes are stored as alternate nodes in the event of a link failure.

(iv) RREQ message is sent to the selected node and the selected node receives RREQ message. It forwards the same on the available active route.

(v) The destination node D sends back RREP on the reverse path. When S receives RREP, it means route is established and data is forwarded over the established route.

V. Performance Metrics

RFC 2501 describes a number of quantitative metrics that can be used for evaluating the performance of a routing protocol for mobile wireless ad-hoc networks. Some of these quantitative metrics [3, 35] are defined as follow:

a) Packet Delivery Fraction (PDF)

The packet delivery fraction is defined as the ratio of number of data packets received at the destinations over the number of data packets sent by the sources as given in equation (1). This performance metric is used to determine the efficiency and accuracy of MANET's routing protocols.

$$\text{Packet Delivery Fraction} = \frac{\text{Total Data Packets Received}}{\text{Total Data Packets Sent}} \times 100 \quad (1)$$

b) Average End-to-End Delay (AE2ED)

This is the average time involved in delivery of data packets from the source node to the destination node. To compute the average end-to-end delay, add every delay for each successful data packet delivery and divide that sum by the number of successfully received data packets as given in equation (2). This metric is important in delay sensitive applications such as video and voice transmission.

$$\text{Average End to End Delay} = \frac{\sum (\text{Time Received} - \text{Time Sent})}{\text{Total Data Packets Received}} \quad (2)$$

c) Network Throughput

A network throughput is the average rate at which message is successfully delivered between a destination node (receiver) and source node (sender). It is also referred to as the ratio of the amount of data received from its sender to the time the last packet reaches its destination. Throughput can be measured as bits per second (bps), packets per second or packet per time slot. For a network, it is required that the throughput is at high-level. Some factors that affect MANET's throughput are unreliable communication, changes in topology, limited energy and bandwidth.

d) Normalized Routing Load (NRL)

The normalized routing load is defined as the fraction of all routing control packets sent by all nodes over the number of received data packets at the destination nodes. In other words, it is the ratio between the total numbers of routing packets sent over the network to the total number of data packets received as given in equation (3). This metric discloses how efficient the routing protocol is. Proactive protocols are expected to have a higher normalized routing load than reactive ones. The bigger this fraction is the less efficient the protocol.

$$\text{Normalized Routing Load} = \frac{\text{Total Routing Packets Sent}}{\text{Total Data Packets Received}} \quad (3)$$

e) Packet Loss (PL)

Packet loss occurs when one or more packets being transmitted across the network fail to arrive at the destination. It is defined as the number of packets dropped by the routers during transmission. It can be shown by equations (4) to (6).

$$\text{Packet Loss} = \text{Total Data Packets Dropped} \quad (4)$$

$$\text{Packet Loss} = \text{Total Data Packets Sent} - \text{Total Data Packets Received} \quad (5)$$

$$\text{Packet Loss (\%age)} = \frac{\text{Total Packets Dropped}}{\text{Total Data Packets Sent}} \times 100 \quad (6)$$

In this research paper, performance of the proposed protocol EESSRP has been evaluated w.r.t. SSRP and AODV.

VI. Simulation Model

An effort has been carried out to develop a new protocol, EESSRP (Energy Efficient, Secure and Stable Routing Protocol). This protocol provides energy-efficient, secured and stable routing strategy for mobile ad hoc networks. The results have been derived by writing a *tcl* script and generating corresponding *trace* and *nam* files. Varying number of UDP connections/traffic agents have been used to analyze the traffic. The mobility model used is random waypoint model in a square area. The area configurations used are 750 meter x 750 meter for 20 nodes, 1000 meter x 1000 meter for 50 nodes and 1500 meter x 1500 meter for 80 nodes. The packet size is 512 bytes. The simulation run time is 500 seconds during analysis of 20 nodes, 700 seconds for 50 nodes and 950 seconds for 80 nodes. All simulation parameters have been summarized below in table 1.

Table 1: Simulation Parameters during analysis of EESSRP

Simulation Software	NS-2.34		
Channel	Wireless		
Mobility Model	Random Waypoint		
Frequency	915e+6		
Transmitted Signal Power	0.2818 W		
Power Consumption for Transmission	1.6 W		
Power Consumption for Reception	1.2 W		
Threshold	10 db		
System Loss Factor	1.0		
Data Rate	1 mbps		
Protocols	AODV, SSRP and EESSRP		
Packet size	512 byte		
Transmission Range	200 meter		
Traffic Agent	UDP		
Queue Length	150		
Number of Nodes	20	50	80
Simulation Time (seconds)	500	700	950
Area	750 × 750	1000 × 1000	1500 × 1500
Fixed Speed (meter/second)	5	5	5
Pause time (seconds)	100 to 500	100 to 500	100 to 950

a) Snapshots of Simulation Environment

An extensive simulation model having scenario of 20, 50 and 80 mobile nodes is used to study inter-layer interactions and their performance implications. Same scenario has been used for performance evaluation of EESSRP, SSRP and AODV protocols at one time. Some of the snapshots of trace and NAM files created using AODV, SSRP and EESSRP protocols for 50 nodes are shown in figure 1 to 6.

```
+ -t 3.000000000 -s 0 -d -1 -p AODV -e 48 -c 2 -a 0 -i 0 -k RTR
- -t 3.000000000 -s 0 -d -1 -p AODV -e 48 -c 2 -a 0 -i 0 -k RTR
h -t 3.000000000 -s 0 -d -1 -p AODV -e 48 -c 2 -a 0 -i 0 -k RTR
+ -t 3.000115000 -s 0 -d -1 -p AODV -e 106 -c 2 -a 0 -i 0 -k MAC
- -t 3.000115000 -s 0 -d -1 -p AODV -e 106 -c 2 -a 0 -i 0 -k MAC
h -t 3.000115000 -s 0 -d -1 -p AODV -e 106 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963291 -s 9 -d -1 -p AODV -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963308 -s 40 -d -1 -p AODV -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963329 -s 20 -d -1 -p AODV -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963360 -s 10 -d -1 -p AODV -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963394 -s 30 -d -1 -p AODV -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963397 -s 11 -d -1 -p AODV -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963397 -s 21 -d -1 -p AODV -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963441 -s 4 -d -1 -p AODV -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963467 -s 1 -d -1 -p AODV -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963504 -s 15 -d -1 -p AODV -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963534 -s 19 -d -1 -p AODV -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963558 -s 24 -d -1 -p AODV -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963641 -s 7 -d -1 -p AODV -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963646 -s 35 -d -1 -p AODV -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963738 -s 43 -d -1 -p AODV -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963741 -s 2 -d -1 -p AODV -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963760 -s 37 -d -1 -p AODV -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963763 -s 8 -d -1 -p AODV -e 48 -c 2 -a 0 -i 0 -k MAC
```

Figure 1: NAM File using AODV (50 Nodes)

```
s 3.000000000 _0_ AGT  --- 0 cbr 512 [0 0 0 0] ------- [0:0 1:0 32 0] [0] 0 0
r 3.000000000 _0_ RTR  --- 0 cbr 512 [0 0 0 0] ------- [0:0 1:0 32 0] [0] 0 0
s 3.000000000 _0_ RTR  --- 0 AODV 48 [0 0 0 0] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
s 3.000115000 _0_ MAC  --- 0 AODV 106 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963291 _9_ MAC  --- 0 AODV 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963308 _40_ MAC  --- 0 AODV 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963329 _20_ MAC  --- 0 AODV 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963360 _10_ MAC  --- 0 AODV 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963394 _30_ MAC  --- 0 AODV 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963397 _11_ MAC  --- 0 AODV 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963397 _21_ MAC  --- 0 AODV 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963441 _4_ MAC  --- 0 AODV 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963467 _1_ MAC  --- 0 AODV 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963504 _15_ MAC  --- 0 AODV 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963534 _19_ MAC  --- 0 AODV 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963558 _24_ MAC  --- 0 AODV 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963641 _7_ MAC  --- 0 AODV 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963646 _35_ MAC  --- 0 AODV 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963738 _43_ MAC  --- 0 AODV 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963741 _2_ MAC  --- 0 AODV 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963760 _37_ MAC  --- 0 AODV 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963763 _8_ MAC  --- 0 AODV 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963776 _49_ MAC  --- 0 AODV 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963787 _13_ MAC  --- 0 AODV 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
```

Figure 2: Trace File using AODV (50 nodes)

```
+ -t 3.000115000 -s 0 -d -1 -p SSRP -e 106 -c 2 -a 0 -i 0 -k MAC
- -t 3.000115000 -s 0 -d -1 -p SSRP -e 106 -c 2 -a 0 -i 0 -k MAC
h -t 3.000115000 -s 0 -d -1 -p SSRP -e 106 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963291 -s 9 -d -1 -p SSRP -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963308 -s 40 -d -1 -p SSRP -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963329 -s 20 -d -1 -p SSRP -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963360 -s 10 -d -1 -p SSRP -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963394 -s 30 -d -1 -p SSRP -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963397 -s 11 -d -1 -p SSRP -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963397 -s 21 -d -1 -p SSRP -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963441 -s 4 -d -1 -p SSRP -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963467 -s 1 -d -1 -p SSRP -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963504 -s 15 -d -1 -p SSRP -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963534 -s 19 -d -1 -p SSRP -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963558 -s 24 -d -1 -p SSRP -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963641 -s 7 -d -1 -p SSRP -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963646 -s 35 -d -1 -p SSRP -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963738 -s 43 -d -1 -p SSRP -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963741 -s 2 -d -1 -p SSRP -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963760 -s 37 -d -1 -p SSRP -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963763 -s 8 -d -1 -p SSRP -e 48 -c 2 -a 0 -i 0 -k MAC
r -t 3.000963776 -s 49 -d -1 -p SSRP -e 48 -c 2 -a 0 -i 0 -k MAC
```

Figure 3 : NAM File using SSRP (50 Nodes)

```
r 3.000963291 _9_ MAC  --- 0 SSRP 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963308 _40_ MAC  --- 0 SSRP 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963329 _20_ MAC  --- 0 SSRP 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963360 _10_ MAC  --- 0 SSRP 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963394 _30_ MAC  --- 0 SSRP 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963397 _11_ MAC  --- 0 SSRP 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963397 _21_ MAC  --- 0 SSRP 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963441 _4_ MAC  --- 0 SSRP 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963467 _1_ MAC  --- 0 SSRP 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963504 _15_ MAC  --- 0 SSRP 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963534 _19_ MAC  --- 0 SSRP 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963558 _24_ MAC  --- 0 SSRP 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963641 _7_ MAC  --- 0 SSRP 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963646 _35_ MAC  --- 0 SSRP 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963738 _43_ MAC  --- 0 SSRP 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963741 _2_ MAC  --- 0 SSRP 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963760 _37_ MAC  --- 0 SSRP 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963763 _8_ MAC  --- 0 SSRP 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963776 _49_ MAC  --- 0 SSRP 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963787 _13_ MAC  --- 0 SSRP 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963817 _3_ MAC  --- 0 SSRP 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000963820 _6_ MAC  --- 0 SSRP 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
r 3.000988291 _9_ RTR  --- 0 SSRP 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]] (REQUEST)
```

Figure 4: Trace File using SSRP (50 Nodes)

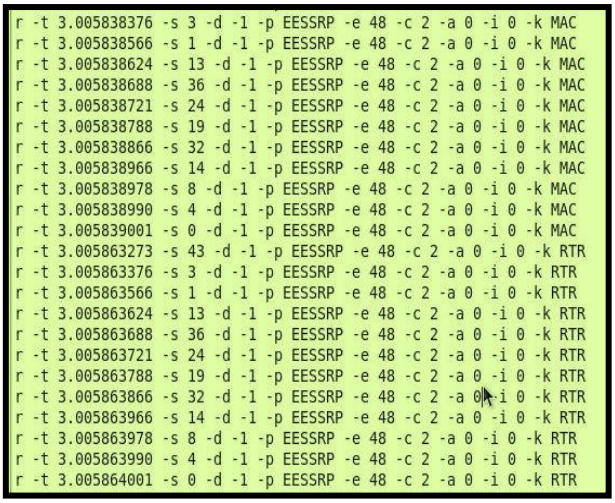

Figure 5 : NAM File using EESSRP (50 Nodes)

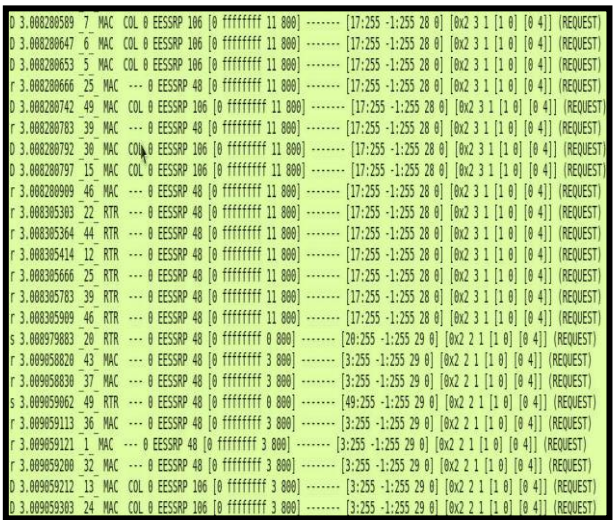

Figure 6 : Trace File using EESSRP (50 Nodes)

A graphical tool known as Network Animator is used to observe the visual representation of NAM files created during simulation of 50 nodes. The snapshots of visual representations taken at two different times t_1= 138.942153 Sec. and t_2= 138.974673 Sec. are given in figure 7 and 8.

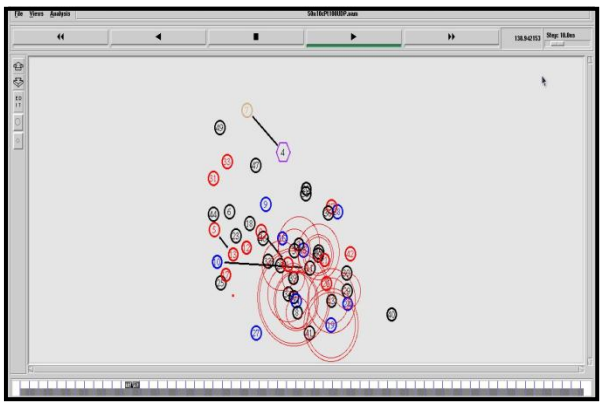

Figure 7 : Position at time t_1= 138.942153 Seconds (50 Nodes)

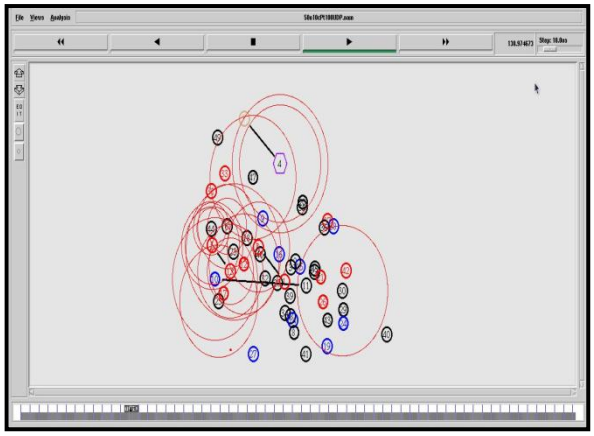

Figure 8 : Position at time t_2= 138.974673 Seconds (50 Nodes)

b) Simulation Results for 20 Nodes

All the performance metrics have been evaluated for EESSRP, SSRP and AODV protocols using 6 UDP connections. All nodes are moving at a fixed speed of 5 meters/second. Two malicious nodes have been introduced in the network scenarios which are moving at a speed of 1 meter/second. The pause time has been used as a varying parameter from 100 seconds to 500 seconds and the queue length is 150.

Figure 9 shows packet delivery fraction with respect to pause time. The observation is that EESSRP and SSRP gives almost same PDF but it is high than that of AODV. Therefore, EESSRP protocol outperforms AODV in terms of energy-efficient, secured and stable routing over MANET. In figure 10, average end to end delay has been presented with respect to pause time. When the pause time is 100 seconds, AODV has high average end to end delay than SSRP and EESSRP but after that AODV, SSRP and EESSRP gives almost same results. On an average, EESSRP outperforms AODV. The network throughput with respect to pause time has been shown in figure 11. The protocol having high network throughput is more efficient and in this figure, EESSRP gives high throughput than SSRP and SSRP gives high throughput than AODV. Therefore, EESSRP outperforms AODV and SSRP in terms of throughput. Figure 12 shows normalized routing load by varying pause time. The bigger this fraction is the less efficient the routing protocol. When the pause time is between 100 seconds to 300 seconds, AODV shows bigger NRL than SSRP and EESSRP but after that EESSRP, SSRP and AODV gives almost same results. On an average, EESSRP outperforms AODV and SSRP in terms of normalized routing load. In figure 13, the packet loss has been shown for both protocols. Higher the packet loss, less efficient is routing protocol and in this figure, AODV gives high packet loss than SSRP and EESSRP. Therefore, EESSRP outperforms than AODV and SSRP in terms of packet loss.

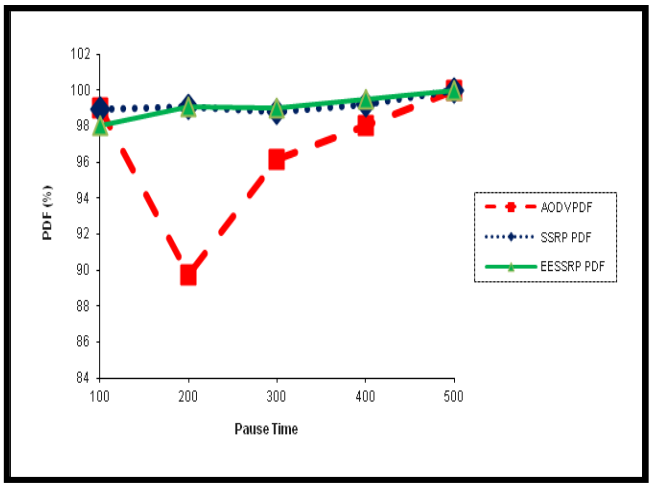

Figure 9 : Packet Delivery Fraction (20 Nodes)

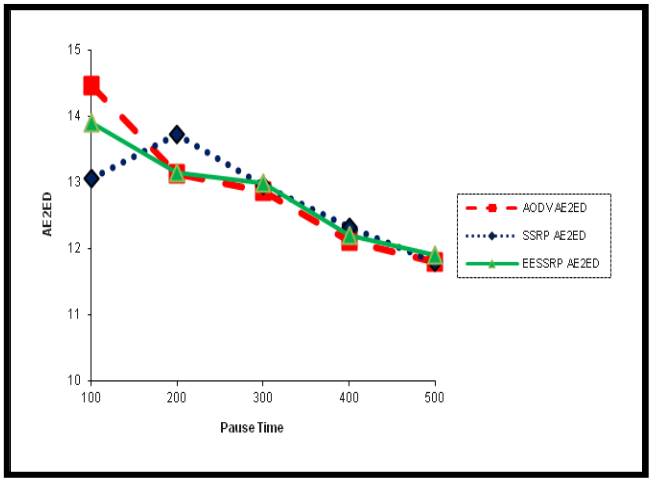

Figure 10 : Average End to End Delay (20 Nodes)

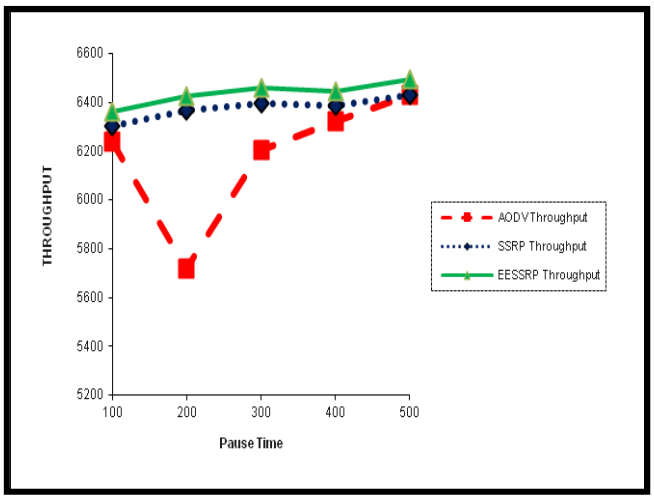

Figure 11: Network Throughput (20 Nodes)

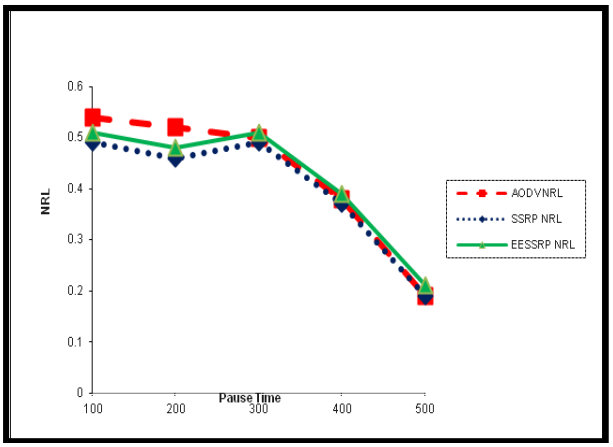

Figure12 : Normalized Routing Load (20 Nodes)

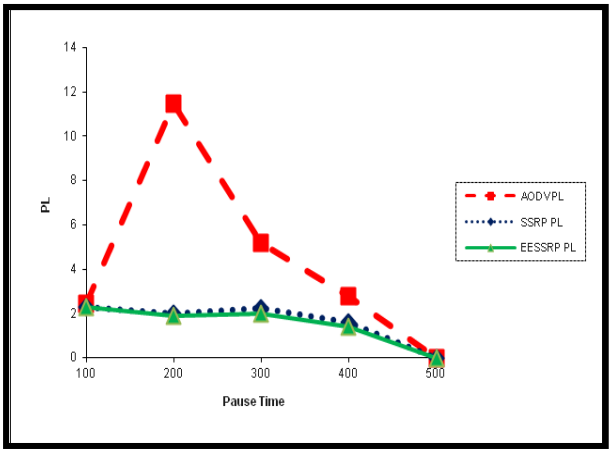

Figure 13 : Packet Loss (20 Nodes)

c) Simulation Results for 50 Nodes

All the performance metrics have been evaluated for EESSRP, SSRP and AODV protocols using 10 UDP connections. All nodes are moving at a fixed speed of 10 meters/second. Two malicious nodes have been introduced in the network scenarios which are moving at a speed of 5 meters/second. The pause time has been used as a varying parameter from 100 seconds to 700 seconds and the queue length is 150.

In figure 14, packet delivery fraction is shown with respect to pause time for EESSRP, SSRP and AODV. The observation is that EESSRP gives high packet delivery fraction that SSRP and SSRP gives high packet delivery fraction that AODV. Therefore, EESSRP protocol outperforms AODV in terms of better packet delivery.

In figure 15, average end to end delay has been presented with respect to pause time. When the pause time is between 100 seconds to 200 seconds, AODV has high average end to end delay than SSRP and EESSRP. When pause time is between 200 seconds to 400 seconds, EESSRP and SSRP has high average end to end delay than AODV. In end, when pause time is between 400 seconds to 500 seconds, EESSRP and SSRP has low average end to end delay than AODV.

Therefore, on an average, EESSRP almost touches AODV. Network throughput with respect to pause time has been shown in figure 16. EESSRP gives high throughput than SSRP and AODV. Therefore, EESSRP outperforms SSRP and AODV in terms of throughput.

Figure 17 shows normalized routing load by varying pause time. When the pause time is between 100 seconds to 300 seconds, AODV shows higher normalized routing load than SSRP and EESSRP but when the pause time is between 300 seconds to 400 seconds, EESSRP gives higher normalized routing load than SSRP and AODV. In end, EESSRP, SSRP and AODV give almost same results. Concluding, it is inferred that EESSRP outperforms AODV in terms of normalized routing load.

In figure 18, AODV shows high packet loss than SSRP and EESSRP. Therefore, EESSRP outperforms than AODV and SSRP.

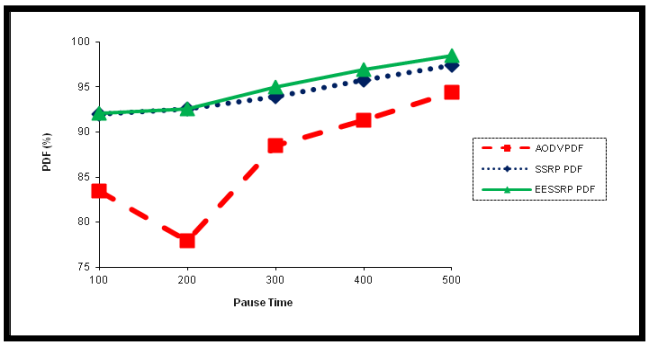

Figure 14 : Packet Delivery Fraction (50 Nodes)

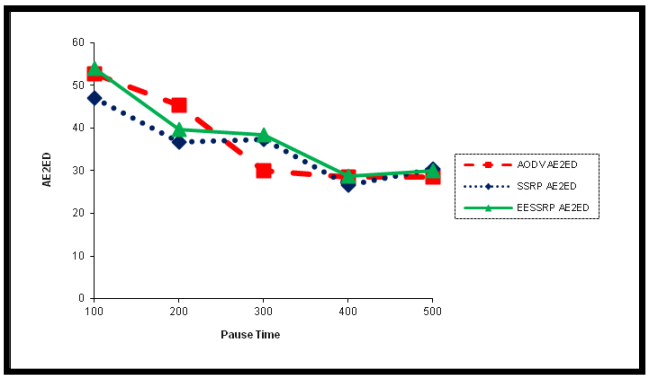

Figure 15 : Average END to End Delay (50 Nodes)

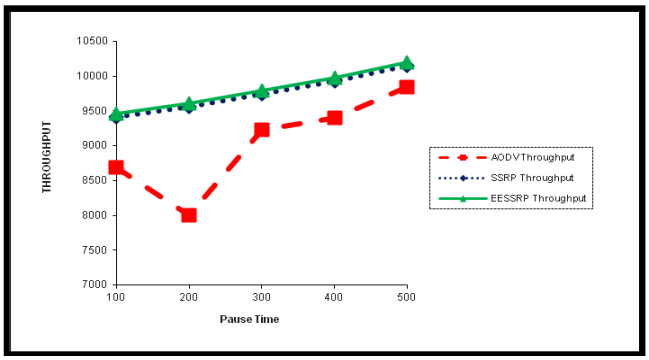

Figure 16 : Network Throughput (50 Nodes)

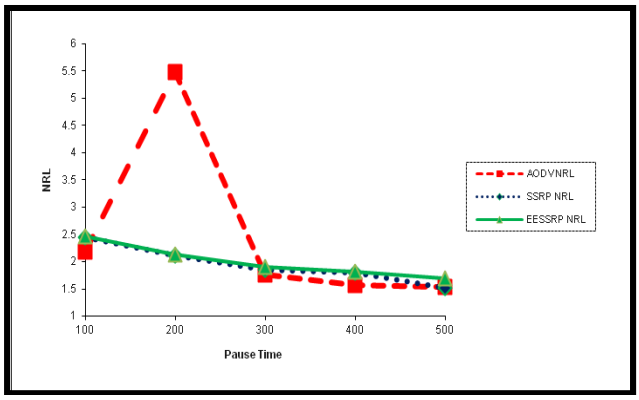

Figure 17 : Normalized Routing Load (50 Nodes)

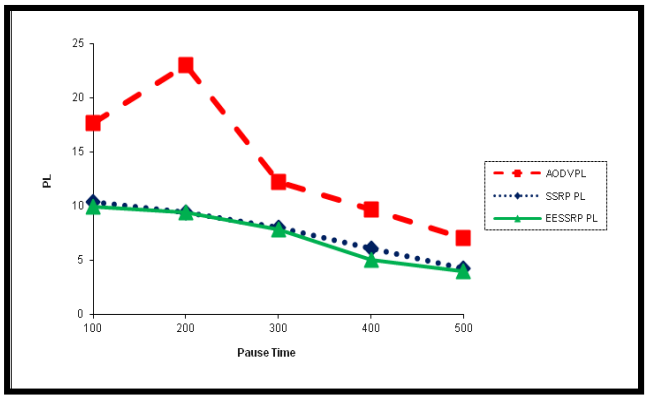

Figure 18 : Packet Loss (50 Nodes)

d) Simulation Results for 80 Nodes

All the performance metrics have been evaluated for EESSRP, SSRP and AODV protocols using 14 UDP connections. All nodes are moving at a fixed speed of 10 meters/second. Two malicious nodes have been introduced in the network scenarios which are moving at a speed of 5 meters/second. The pause time has been used as a varying parameter from 100 seconds to 950 seconds and the queue length is 150.

Figure 19 shows that packet delivery fraction for EESSRP and SSRP is much higher than that of AODV for all pause times and hence EESSRP outperforms AODV and SSRP in terms of better packet delivery. In figure 20, average end to end delay has been presented with respect to pause time. When the pause time is between 100 seconds to 675 seconds, AODV has high average end to end delay than SSRP and EESSRP but when it is between 675 seconds to 950 seconds, EESSRP and SSRP gives high average end to end delay than AODV. Concluding EESSRP outperforms AODV and SSRP initially but in end AODV starts outperforming SSRP and EESSRP. This issue is still under consideration. Network throughput with respect to pause time has been shown in figure 21. EESSRP gives high throughput than AODV and SSRP for all pause times and hence EESSRP outperforms AODV and SSRP in terms of better throughput.

Figure 22 shows normalized routing load by varying pause time. The bigger this fraction is the less efficient the routing protocol. When the pause time is between 100 seconds to 250 seconds, EESSRP and SSRP shows bigger NRL than AODV; when it is between 250 seconds to 400 seconds, AODV shows bigger NRL than SSRP and EESSRP. When pause time is between 400 seconds to 950 seconds, EESSRP and SSRP shows marginal bigger NRL than AODV. Although both the protocols give almost same results but still due to marginal difference between the results, on an average, AODV outperforms SSRP and EESSRP. In figure 23, the packet loss has been shown for both protocols with respect to varying pause time from 100 seconds to 950 seconds. In all cases, EESSRP gives very low packet loss than AODV and SSRP. So EESSRP outperforms AODV and SSRP.

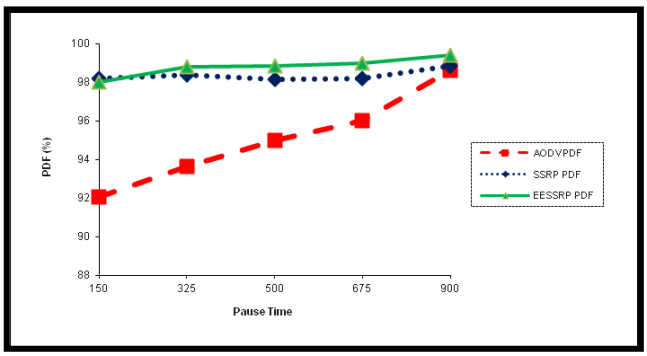

Figure 19 : Packet Delivery Fraction (80 Nodes)

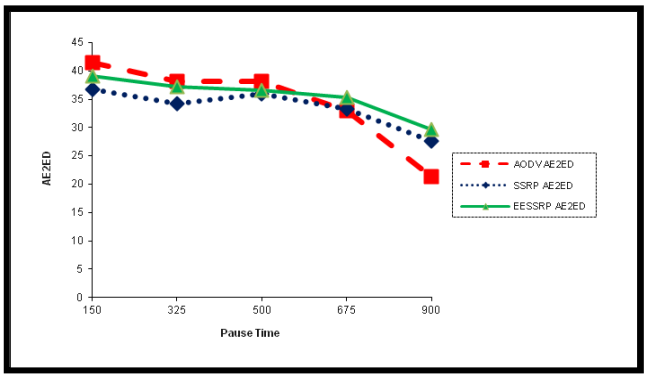

Figure 20 : Average End to End Delay (80 Nodes)

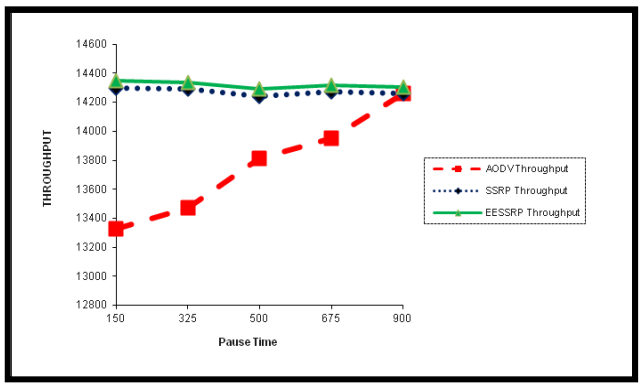

Figure 21 : Network Throughput (80 Nodes)

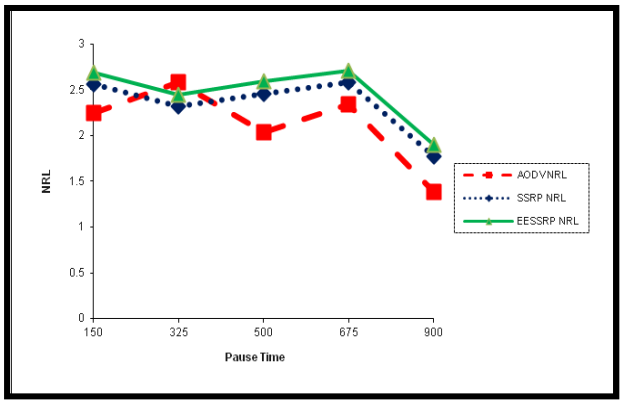

Figure 22 : Normalized Routing Load (80 Nodes)

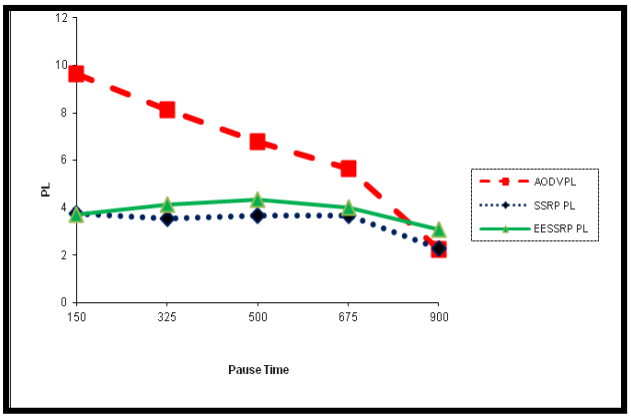

Figure 23 : Packet Loss (80 Nodes)

VII. Conclusion and Future Scope

Results have been derived from a series of experiments conducted on network simulator NS-2.34. The following conclusions have been made:

a) Energy Efficient

The proposed protocol, EESSRP, provides energy efficient routing over mobile adhoc networks in a very efficient way. It assumes that all nodes are capable of dynamically adjusting the transmission power used to communicate with other nodes. Battery power of a node is a precious resource that has been used efficiently in order to avoid early termination of a node or a network. The optimal route selection between source and destination is done on the basis of proper energy management. The proposed protocol balances energy efficient broadcast schemes in ad hoc network and maintains connectivity of mobile nodes.

b) Multifold Security Solution

The existing routing protocols are typically attack-oriented. They first identify the security threats and then enhance the existing protocol to conquer such attacks. Since the solutions are designed explicitly with certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks. Therefore, a multifold network security solution has been developed in EESSRP that

offers multiple lines of defense against both known and unknown security threats and the performance of same has been evaluated with respect to AODV using various performance metrics viz. packet delivery fraction, average end to end delay, network throughput, normalized routing load and packet loss.

c) Robust and Stable

EESSRP satisfies the condition. It has been thoroughly checked many times using different scenes and changing loads. Since routers are located at different points, they can cause considerable problems when they fail. The proposed protocol takes care of the issue. The best routing algorithms is often the one that withstands the test of time and that proves stable under a variety of network conditions.

d) Best Packet Delivery Ratio

EESSRP is the best in terms of packet transmission. More packets are transmitted than any of the studied protocols. This is true even in case of changing scenario and fast moving nodes. So it is able to achieve one of the most important objectives of ad hoc networks as successful packet delivery.

e) Optimal Path

EESSRP selects the optimum path. Routing protocols use metrics to evaluate what path will be the best for a packet to travel. Using routing table entries and making choice between active and week nodes, it is able to select a path that is stable. This proves the optimality of the protocol.

f) Simple

EESSRP can easily be implemented and executed. The simulation studies have been conducted on Pentium-IV with standard configurations. Though it is best performing under Linux environment but can be easily implemented on Windows platform also. Efficiency is particularly important when the software implementing the routing algorithm must run on a computer with limited physical resources. PAVNR suffices the purpose easily.

g) Rapidly Converging

EESSRP converges nicely and quickly. In all simulations, problem of looping never occurred. *Convergence* is the process of agreement, by all routers, on optimal routes. Slow convergence can cause routing loops or network outages.

h) Flexible

When a network segment gets down, as in the case of best protocols, EESSRP become aware of the problem and quickly selects the next-best path for all routes normally using that segment. It quickly and accurately adapt to a variety of network circumstances. It has been nicely programmed to adapt to changes in network bandwidth, router queue size, and network delay etc.

i) Minimum Route Computation and Overhead

EESSRP carries out this issue satisfactorily. Route computation should not involve the maintenance of global state, or even significant amounts of volatile non-local state. Also each node must only care about the routes corresponding to its destination, and must not be involved in frequent topology updates for parts of the network to which it has no traffic.

j) Route Repair

The route repair phase of EESSRP is unique as compared to other such protocols and outperform all in its category. It describes the maintenance process, which can be done as fast as possible. It describes the level of self organization in a network. The protocol uses local route repair of routing process.

k) Applicable

Many of the existing models on paper can go wayward in real life situations. Simulations of the EESSRP indicate its worth in real life scenarios as well.

VIII. Future Scope for Researchers

Ad hoc network routing research is still in progress. Outcome of the current research has exhibited the possibilities of further extensions. Some of the research work that can be carried out in future as an extension of current work is given below:

a) EESSRP should support Metropolitan area wireless ad hoc networking. For a real map, high number of nodes and suitable radio interface, a realistic earthquake scenario could be generated. The scenario considered is representing a maximum area of 1.5 KM square. Metropolitan area networking may require more area to be covered.

b) It should check the cases when nodes may be given less energy, so that partitioning behavior could be observed for different routing protocols. The nodes are given power status large enough to survive transmission. The other case may be taken when most of the nodes have depleting power factor. The effect of protocol may be checked in those cases.

c) It should support enhanced TCP connections. A transmission control protocol which is mobility enhanced [GOF00] could be implemented and used. In enhanced TCP connection, nodes are able to change speed while moving in the scenario and start moving at a new speed.

d) It should provide quality of service (QoS) [CHA01, MIR01, RAO98, SAJ00], which should be embedded in routing protocol. QoS is the ability of a network element (e.g. an application, host or router) to have some level of assurance often given in

terms of bandwidth or delay. It should be able to provide satisfactorily the level of Qos desired.

e) It should be able to handle cellular techniques, which could include the hand-over technique used for cellular networks [PER95, SCO97]. When a cellular phone moves from one cell to the other, the Base Station (BS) will detect this from the signal power and inform the Mobile Switching Centre (MSC) of that. The MSC will then switch the control of the call to the BS of the new cell, where the phone is located. This is called handover.

f) It should be able to work nicely for fading problems [PER95, SCO97]. Fading is the reduction of signal power. Fading is caused by many factors - the most important ones being multipath and shielding. Multipath fading is caused by the transmission of the signal along different paths and resulting in simultaneous reception. Depending of the amplitudes and phase of the signal, the result of this could be that the signals cancel each other completely or significant attenuation in the resultant signal. Shielding is the absence of field strength. Most common causes are tunnels, hills and inside certain buildings.

g) It should make use of diversity coding technique. The proposed protocol is an enhanced version of AODV. It has not been tested for source routing. An experiment may be conducted to check the performance of EESSRP for source routing also.

h) It should be able to support multicast transmission. Multicasting [GER00, PAU98, ROY99] is the transmission of packets to a group of hosts identified by a single destination address. Multicasting is intended for group-oriented computing. There are three primary functions that must be performed to implement IP multicasting: addressing, group management, and datagram processing / routing. It minimizes the link bandwidth consumption, sender and router processing, and delivery delay.

i) It should be able to increase the number of mobile nodes and to introduce more malicious nodes in the network scenario so that its impact on the network performance may be determined. The efforts can be made in the direction of improving hash functions to avoid collisions, using stronger hash keys by making them dependent on additional parameters like biometric credentials, passwords, IP addresses etc.

j) It should handle Mobile-IP [http:ENW, http:CIS]. Mobile IP provides users the freedom to roam beyond their home subnet while consistently maintaining their home IP address. This enables transparent routing of IP packets to mobile users during their movement, so that data sessions can be initiated to them while they roam; it also enables sessions to be maintained in spite of physical movement between points of attachment to the Internet or other networks.

k) It should be tested for fixed networks also. Also there should be a mechanism using a special addressing suitable for separation and merging of ad hoc networks.

References Références Referencias

1. Kush and S. Taneja, "Secured Routing over MANET with Power Management", Advances in Computing and Artificial Intelligence 2011, India, ACM Publisher, USA, pp. 144-149, 2011.
2. T. Karygiannis and L. Owens, "Wireless Network Security", NIST Special Publication, 800-48, November 2002.
3. S. Taneja and A. Kush, "Stable and Secured Routing Strategy for MANET with SSRP", Global Journal of Computer Science & Technology, USA, Volume 12, Issue 4, Version 1.0, pp. 20-32, 2012..
4. Kush A, Gupta P, "Power Aware Virtual Node Routing Protocol for Adhoc Networks", In International Journal of Ubiquitous Computing and Communication (UBICC), Vol 2 No. 3, pp55-62, South Korea 2007.
5. C. Parkins and E. Royer, "Adhoc on demand distance vector routing", 2nd IEEE workshop on Mobile Computing , pages 90-100, 1999
6. Chiasserini C. F., Chlamtac I., Monti P. and Nucci A., "Energy Efficient Design of Wireless Ad hoc Networks", Proceedings of Networking 02, pp. 376-386, 2002.
7. Adamou M. and Sarkar S., "A Framework for Optimal Battery Management for Wireless Nodes", Proceedings of IEEE INFOCOMP, pp. 1783-1792, 2002.
8. Chiasserini C.F. and Rao R.R., "Energy Efficient Battery Management", Proceedings of IEEE INFOCOM'00, vol. 2, pp. 396-403, 2000.
9. Kawadia V. and Kumar P. R., "Power Control and Clustering in Ad hoc Networks", Proceedings of IEEE INFOCOM'03, pp. 459-469, 2003.
10. Toh C. K., "Maximum Battery Life Routing to Support Ubiquitous Mobile Computing in Wireless Ad hoc Networks", IEEE Communications Magazine, vol. 39, No. 6, pp. 138-147, 2001.
11. Singh S., Woo M. and Raghavendra C. S., "Power-Aware Routing in Mobile Ad hoc Networks", Proceedings of ACM/IEEE International Conference on Mobile Computing and Networking, pp. 181–190, 1998.
12. Zheng R. and Kravets R., "On Demand Power Management for Ad hoc Networks", Proceedings of IEEE INFOCOMP, vol. 1, pp. 481-491, 2003.
13. Toh C. K., "Maximum Battery Life Routing to Support Ubiquitous Mobile Computing in Wireless

Ad hoc Networks", IEEE Communications Magazine, vol. 39, No. 6, pp. 138-147, 2001.
14. A. Kush, P. Gupta, and R. Chauhan, "**Stable and Energy Efficient Routing for Mobile Ad hoc Networks",** 5th International Conference on Information Technology: New Generations (ITNG), Las Vegas, USA, IEEE explore, DOI 10.1109/ITNG.2008.230, pp. 1028-1033, 2008.
15. Luo J. and Jha N. K., "Battery Aware Static Scheduling for Distributed Real Time Embedded Systems", Proceedings of IEEE DAC, pp. 444-449, 2001.
16. Li P.et al., "Power Control Network Protocol for Multirate Ad hoc Network", IEEE Transaction on Wireless Communications, Vol. 8, No. 4, pp. 2142-2148, 2009.
17. Chang J. H. and Tassiulas L. "Energy Conserving Routing in Wireless Ad hoc Networks", Proceedings of IEEE INFOCOM'00, pp. 22-31, 2000.
18. Wu J., Dai F., Gao M. and Stojmenovic I. , "On Calculating Power Aware Connected Dominating Set for Efficient Routing in Ad hoc Wireless Networks", IEEE/KICS Journal of Communication Networks, Vol. 4, No. 1, pp. 59-70, 2002.
19. Xue Y. and Li B., "A Location added Power Aware Routing Protocol in Mobile Ad hoc Networks", Proceedings of IEEE GLOBECOM'01, pp. 2837-2841, 2001.
20. Domingo M.C., Remondo D. and Leon O., "A Simple Routing Scheme for Improving Ad hoc Network Survivability", Proceeding IEEE GLOBECOM'03, pp. 718-723, 2003.
21. Laura Sanchez et al., "Energy and Delay-Constrained Routing in Mobile Ad hoc Networks: An Initial Approach", Proceedings of ACM International Workshop on Performance Evaluation of Wireless Ad hoc, Sensor and Ubiquitous Networks, pp. 262-263, 2005.
22. Chen Jie et al., "Energy Efficient AODV for Low Mobility Ad hoc Networks', Proceedings of Wireless Communications", Networking and Mobile Computing Conference (WiCom'07), pp. 1512-1515, 2007.
23. Senouci S. M. and Naimi M., "New Routing for Balanced Energy Consumption in Mobile Ad hoc Networks", Proceedings of ACM International Workshop on Performance Evaluation of Wireless Ad hoc, Sensor and Ubiquitous Networks, pp. 238-241, 2005.
24. Narayanaswami S., Kawadia V., Srinivas R. S. and Kumar P.R., "Power Control in Ad hoc Networks: Theory, Architecture, Algorithm and Implementation of the COMPOW Protocol", Proceedings of European Wireless Conference, pp. 156-162, 2002.
25. Xue Y. and Li B., "A Location added Power Aware Routing Protocol in Mobile Ad hoc Networks", Proceedings of IEEE GLOBECOM'01, pp. 2837-2841, 2001.
26. T. Karygiannis and L. Owens, "Wireless Network Security", NIST Special Publication, 2002.
27. William Stallings, "Cryptography and Network Security: Principles and Practice", Prentice Hall, 5th Edition, 2011.
28. Dahill B., Levine B. N., Royer E. and Shields C., "A secure routing protocol for ad hoc networks", Technical Report UM-CS-2001-037, University of Massachusetts, Department of Computer Science, 2011.
29. Hu Y. C., Johnson D. B., and Perrig A., "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks", Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications, pp. 3-9, IEEE Computer Society, 2002.
30. Papadimitratos P. and Haas Z. J., "Secure routing for mobile ad hoc networks", SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), 2002.
31. Zapata M. G., "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing", IETF MANET Mailing List, Available at ftp://manet.itd.nrl.navy.mil/pub/manet/, 2004.
32. Papadimitratos P. and Haas Z. J., "Secure Link State Routing for Mobile Ad hoc Networks", Proceedings of IEEE Workshop on Security and Assurance in Ad hoc Networks, IEEE Press, pp. 27–31, 2003.
33. Hu Y. C., Perrig A. and Johnson D., "Ariadne: A secure on-demand routing protocol for ad hoc networks", Technical Report TR01-383, Rice University, 2001.
34. Kravets R., Yi S., and Naldurg P., "A Security-Aware Routing Protocol for Wireless Ad hoc Networks", ACM Symposium on Mobile Ad hoc Networking and Computing, 2001.
35. Georgios Kioumourtzis, "Simulation and Evaluation of Routing Protocols for Mobile Ad hoc Networks", Thesis, Master of Science in Systems Engineering and Master of Science in Computer Science, Naval Postgraduate School, Monterey, California, 2005.
36. Kawadia V. and Kumar P. R., "Power Control and Clustering in Ad hoc Networks", Proceedings of IEEE INFOCOM'03, pp. 459-469, 2003.

This page is intentionally left blank