A Secure and Power Efficient Routing Scheme for Ad Hoc Networks

Ashwani Kush
CSE Dept,University College,
Kurukshetra, India

Divya Sharma
IT Dept, ITM University
Gurgaon, India

Sunil Taneja
CSE Dept,Govt. PG college
Kalka, India

ABSTRACT

A recent trend in Ad Hoc network routing is the reactive on-demand philosophy where routes are established only when required. Security and Power efficiency are the major concerns in this field. This paper is an effort to combine these factors of security and power to achieve more reliable routing. Most of the protocols in this category are either incorporating security features or considering power factor. In the study no existing protocol is merging the two factors to see results. The ad hoc environment is accessible to both legitimate network users and malicious attackers. The ad hoc environment has the constraint of power factor. The proposed scheme is intended to incorporate both factors on existing protocols. The study will help in making protocol more robust against attacks and implementing power factor to achieve stable routing in routing protocols

Keywords

MANET, Security, Ad hoc networks, Routing protocols, AODV, Power status.

1. INTRODUCTION

Mobile Ad-Hoc Networks (MANETs) are self-organizing, rapidly deployable, and require no fixed infrastructure. An Ad hoc 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 defense 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 Ad Hoc 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 Ad Hoc environment. The main goal of the security solutions for an Ad Hoc network is to provide security services, such as authentication, confidentiality, integrity, anonymity and availability to mobile users [1,2]. 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 ad hoc 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 Ad hoc 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 ad hoc 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] with power and virtual nodes. The scheme has been incorporated on the refined version of AODV [4]. Rest of the paper is organized as: Section 2 describes types of security attacks and related work. Section 3 deals with Power factor and its related work. Section 4 proposes a new model for security and power. Section 5 is simulations and results and Section 6 concludes the study.

2. SECURITY ATTACKS

In this paper, the prime concern is with the attacks targeting the routing protocols for Ad hoc Networks. These attacks can be broadly classified into two main categories as: Passive attacks, Active attacks.

2.1 Passive Attacks

Passive attacks are the attacks in which an attacker does not actively participate in bringing the network down. An attacker just eavesdrops on the network traffic as to determine which nodes are trying to establish routes, or which nodes are pivotal to proper operation of the network and hence can be potential candidates for subversion and launching denial of service attacks. The attacker can then forward this information to an accomplice who in turn can use it to launch attacks to bring down the network. Some of the generic types of attack [5,6] that might be encountered in passive attacks are:

1. Interruption**:** An asset of the system is destroyed, becomes unavailable or unusable. This is an attack on availability.

2. Interception: An unauthorized party gains access to an asset. This is an attack on confidentiality. The unauthorized party could be a person, a program or a computer.

3. Modification: An unauthorized party tampers with an asset. This is an attack on integrity.

4. Fabrication: An unauthorized party inserts malicious objects into the system.

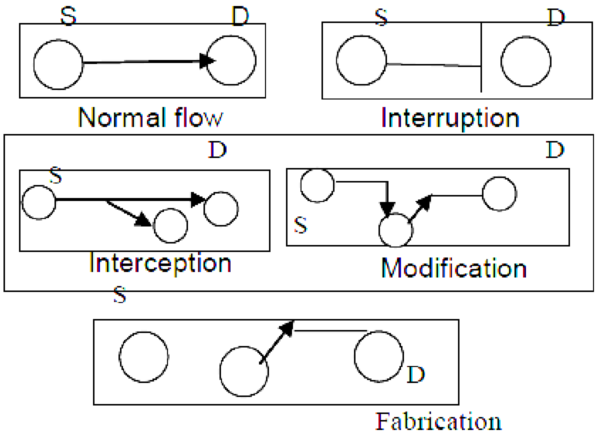

Fig 1. Type of passive attacks

S represents Source and D represents Destination.

2.2 Active Attacks

These attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories.

1. Replacement: In this attack one entity pretends to be a different entity. It is a type of attack that is used by someone familiar with your security procedures and failures.

2. Replay: This involves capture of data units and its subsequent retransmission to produce an unauthorized effect.

3. Modification of Messages: This simply means that some portion of a legitimate message is altered, delayed or reordered.

4. Denial of Service: This prevents the normal use or management of communication facilities.

It is quite difficult to prevent active attacks absolutely, as this would require physical protection of all communications facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them.

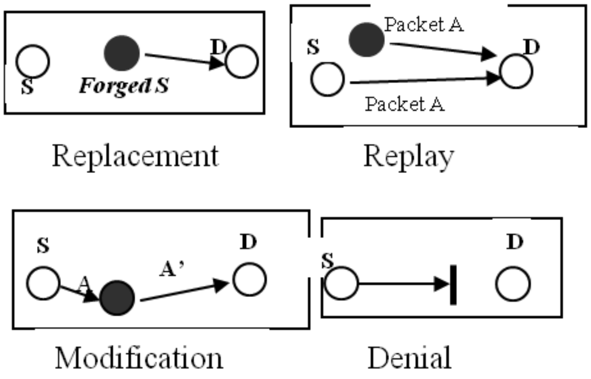

Fig 2: Type of active attacks

Figure 2 represents type of Active attacks, S represents Source and D represents Destination.

2.3 Related Work

Major efforts on security of routing protocols 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. Dahill et al. proposed ARAN [7], it assumes managed-open environment, where there is a possibility for pre-deployment of infrastructure. It consists of two distinct stages. The first stage is the certification and end-to-end authentication stage. Here the source gets a certificate from the trusted certification server, and then using this certificate, signs the request packet. Each intermediate node in turn signs the request with its certificate. The destination then verifies each of the certificates, thus the source gets authenticated and so do the intermediate nodes. The destination node then sends the reply along the route reverse to the one in the request, reply signed using the certificate of the destination. The second stage is a non-mandatory stage used to discover the shortest path to the destination, but this stage is computationally expensive. It is prone to reply attacks using error messages unless the nodes have time synchronization. Haas [8] proposed a protocol (SRP) that can be applied to several existing routing protocols. This protocol assumes a security association between source and destination nodes. Intermediate nodes do not need to cryptographically validate the control traffic. It adds a SRP header to the base routing protocol (DSR or AODV) request packet. SRP header has three important fields—QSEQ which helps prevent replay of old outdated requests, QID and random number which helps prevent fabrication of requests, and a SRP MAC which ensures integrity of the packets in transit. SRP requires that, for every route discovery, source and destination must have a security association between them. Here any malicious node can just forge error messages with other nodes as source. ARIADNE [9], is based on DSR [10] and TESLA [11] (on which is based its authentication mechanism). ARIADNE prevents attackers/compromised nodes from disrupting uncompromised routes comprising of benign nodes. It uses highly efficient symmetric key cryptography. ARIADNE does not guard against passive attackers eavesdropping on the network traffic. It does not prevent an attacker from inserting data packets. ARIADNE is vulnerable to active-1-1 attacker that lies along the discovered route, who does not forward packets and does not generate ERROR if it encounters a broken link. It also requires clock synchronization, which we consider to be an unrealistic requirement for ad hoc networks. Perlman proposed a link state routing protocol [12] that achieves Byzantine Robustness. Although the protocol is highly robust, it requires a very high overhead associated with public key encryption. In their paper on securing ad hoc networks [13], Zhou and Haas primarily discussed key management. They devote a section to secure routing, but essentially conclude that ―nodes can protect routing information in the same way they protect data traffic‖. They also observe that denial-of-service attacks against routing will be treated as damage and routed around. Some work has been done to secure ad hoc networks by using misbehavior detection schemes [14]. This approach has two main problems: first, it is quite likely that it will be not feasible to detect several kinds of misbehaving; and second as no real means to guarantee the integrity and authentication of the routing messages.

3. POWER FACTOR

Ad hoc networks have limited power capabilities mainly owing to the nature of the infrastructure they use. Power required by each mobile host can be classified into two categories as Communication-related power and Non-communication-related power.

Three Layers are involved in communications as

a) Physical layer: Transmission power should be at a minimum level to maintain links. It should allow adapting to changes in transmission environment.

b) Data Link Layer: Energy conservation can be achieved by using effective retransmission request schemes and sleep mode operation. It is important to appropriately determine when and at what power level a mobile host should attempt retransmission. Node's transceiver should be powered off when not in use.

c) Network Layer: In wireless network it is important that the routing algorithm select the best path from the viewpoint of power constraints as part of route stability.

In a MANET, wireless communication involves usage of a transceiver at the source, intermediate, and destination nodes. The transmitter sends control, route request and response, as well as data packets originating at or routed through the transmitting node. The receiver is used to receive data and control packets - some of which are destined for the receiving node and some of which are forwarded.

A wireless network interface has five possible energy consumption states (six including the off state).

a) Transmit state for transmitting data, control and routing packets.

b) Receive state is for receiving data, control and routing packets.

c) In the idle state, which is the default state for ad hoc environment, the interface can transmit or receive packets.

d) The sleep state has extremely low power consumption as the interface can neither transmit nor receive in this state.

e) Lastly, a node can enter a reduced energy discard state while the media carries uninteresting traffic.

The decision to enter the reduced energy discard state is made by the non-destination nodes in the range of the sender. The reduced energy state uses slightly less power than the idle state, but significantly more than that used in the sleep state [3].

3.1 Related Work

Singh et al [15] proposed power-aware routing and discussed different performance metrics. Minimal energy consumption was used in [16]. Chang and Tassiulas [17] also proposed maximizing the life-time of a network when the message rate is known. Their main idea, namely to avoid using low power nodes and choose the short path at the beginning, has inspired the approach described in this paper. The same formula to describe the residual power fraction has been used here. In [18] Gupta and Kumar discussed the critical power at which a node needs to transmit in order to ensure the network connectivity. Energy efficient MAC layer protocols can be found in [19, 20]. Another important study concerns optimizing power consumption during idle time rather than during the time of communicating messages [21]. The work presented in this paper is different from these previous results in that it develops online, hierarchical, and scalable algorithms that do not rely on knowing the message rate and optimize the lifetime of the network. This work is in fact complementary to the results presented in [22]. Combined, efficient ways for dealing with idle time and with communication can lead to powerful power management solutions. More recent developments are based on Direction Forward Routing (DFR) [23]. When an update is received, a node records the ―geographical direction" to where the update came from. When ―predecessor" forwarding fails, the packet is forwarded to the most promising" neighbor in the recorded direction. It is good for denser mediums only. Another change is Admission Control enabled On demand Routing (ACOR)[24]. Without maintaining up-to-date any routing information and exchanging any routing table periodically, or introducing out weighting signaling functions, a route with QoS requirements is created on-demand.

4. SECURITY MODEL

The proposed scheme is based on the hash key chain mechanism. Hash key chains are constructed by using only symmetric cryptographic primitives, namely hash functions. Authentication and integrity can be achieved by using hash key chains. A hash key chain is configured as a recursive chain, where the node first chooses a random key, K1. Subsequent keys are calculated by calculating the one-way hash over the key [28]:

$$K_2 = H[K_1], \quad K_{N-2} = H[K_{n-1}], \quad K_{N-1} = [K_N]$$

To compute any previous key from key K_I where $J < I$ a node uses the equation: $\mathbf{K_j = H_{I-J}[K_I]}$

This equation is used by any node to authenticate any received value on the hash chain. If the computed value matches previous known authentic key value then the received key is authentic. Each node discloses each key of its one-way key chain in a particular order, which is exactly reverse of the order in which the keys were generated. The key disclosure schedule and key generation schedule should be reverse For example if the keys were generated by a node in the order $\mathbf{K_N}$ **;** $\mathbf{K_{N-1}}$ **; …..**$\mathbf{K_1}$**;** $\mathbf{K_0}$ then the node discloses them in the order $\mathbf{K_0}$ **;** $\mathbf{K_1}$ **; ….** $\mathbf{K_N}$ .. The rationale behind having the key disclosure schedule to be reverse of the key generation schedule is that KN of a node is known to all other nodes and in such a situation they should be able to authenticate any subsequent keys that are disclosed. The use of one way hash function allows $\mathbf{K_0}$ **;** $\mathbf{K_1}$ **; ….** $\mathbf{K_{N-1}}$ to be authenticated using K_N but K_N cannot be authenticated using any other key value. Hence the key disclosure schedule and key generation schedule is reverse. The scheme was proposed by Leslie Lamport [25] and also implemented in earlier work [29] by the author.

4.1 Power Model

Each route table has an entry for its power status. Whenever need for a new route arises, nodes with their power status are checked and a route is established. Same process is repeated in route repair phase. Route tables are updated at each Hello interval as in AODV with added entries for power status and security.

Proposed Energy Scheme

Energy consumption of a node after time t is calculated using equation (1):

$$Ec(t) = Nt * \alpha + Nr * \beta \quad \text{--} \quad (1)$$

Where *Ec*(*t*) , energy consumed by a node after time t. *Nt* , no. of packets transmitted by the node after time t. *Nr* , no. of packets received by the node after time t. *α and β* are constant factors having a value between 0 and 1.If E is the initial energy of a node, the residual energy ERes of a node at time t, can be calculated as:

$$E_{Res} = E - Ec(t) \quad \text{---------} \quad (2)$$

Initially source node generates a REQ with *Emin* set to 100 %. All intermediate nodes sets minimum energy level field of *REQ* to their energy level. An intermediate node on receiving REQ, overwrites minimum energy level *Emin* of the REQ packet iff *ERes< Emin*, where *ERes* is the residual energy of the node and is calculated as given in equation (2). Otherwise, *Emin* remains unchanged. Now intermediate node will forward the route request to its neighbors. This process goes on until REQ reaches to the destination.

4.2 Power Model

Hashing and power estimation is done for route request, reply and not in route error and route erasure phases so that less overhead occurs. If in REQ phase an intermediate node cannot satisfy the security and power requirements, the REQ packet is dropped and not forwarded. Arrival of REQ to Destination will ensure a safe path. REP packet contains this security information specified by sender. So additional field is added to REQ and REP packet formats.

1. Source node broadcasts routing request message to its neighbors in order to find a route to destination node.

2. The neighbors of the source node forward the request to their neighbors if the security evaluation and power status on the source node pass its predefined threshold, until either the destination or an intermediate node with a "fresh enough" route to the destination is reached.

3. If some nodes respond that they have fresh enough route to the destination node, Based on the evaluation result and hops of the routes, the source node selects one preferred route.

4. After receiving the data packages, the destination node applies the same method above to reply the confirmation message if the source node requests it. It is not mandatory to use the same route as the source for better security consideration.

5. If within the time slot, the destination's confirmation arrives and can be verified as valid, the source node will continue sending data packages via the underlying route. If the destination's confirmation cannot receive within the preferred time slot, the source node will update its route table and go for local repair.

6. The source node selects the second best route.

5. SIMULATION RESULT

The proposed scheme has been incorporated on AODV with changing its format and adding Power status and Security parameter. At start one parameter is added and then finally both are added and results have been compared. Simulation study has been carried out to study the performance study of proposed protocol. Simulator used for this study is NS 2 [26].

5.1 Result

Graph 1 show the packet delivery ratio based on pause time. The packet delivery ratio is the fraction of successfully received packets, which survive while finding their destination. This performance measure determines the completeness and correctness of the routing protocol. Pause time of 0 means very fast moving nodes and 500 shows minimum movement.

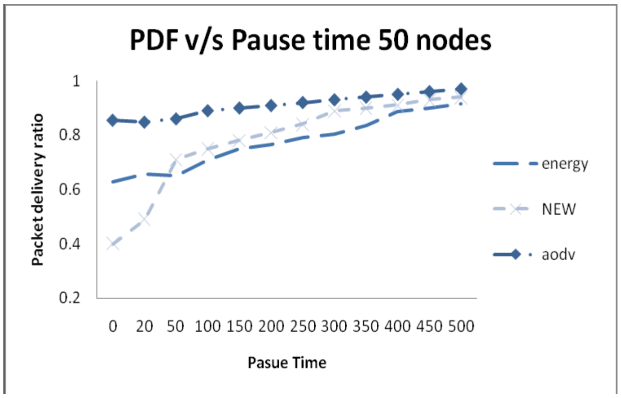

Fig.3: a) PDF using pause time

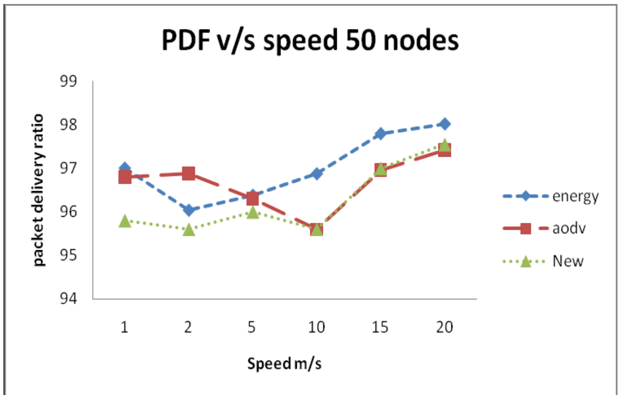

Fig.3: b) PDF using speed as function

As the Graph 1-(a) indicates NEW has less number of packets delivered, but this reduction in delivery is due to Hash keys calculations and Energy check evaluations. AODV without extensions give better results. The study also reveals the ratio is more if only power factor is added; this is due to the fact that mostly nodes are having better battery status initially and less computation is involved. When both factors are joined the hybrid is slightly in between. The start is poor, as computation is maximum at Root discovery start phase and then things stabilize as the pause time is increased. When pause time is approaching 500, NEW achieves almost 98-99% delivery mark. Graph 1-b is the packet delivery ratio with speed as function. As speed increases the delivery drops in all cases. After initial drops, the packet delivery was better when only power factor is added; this phenomenon is still under observation. The delivery drops with added factors of security and power. At higher speed the performance of NEW is good and it is able to touch packet delivery of AODV.

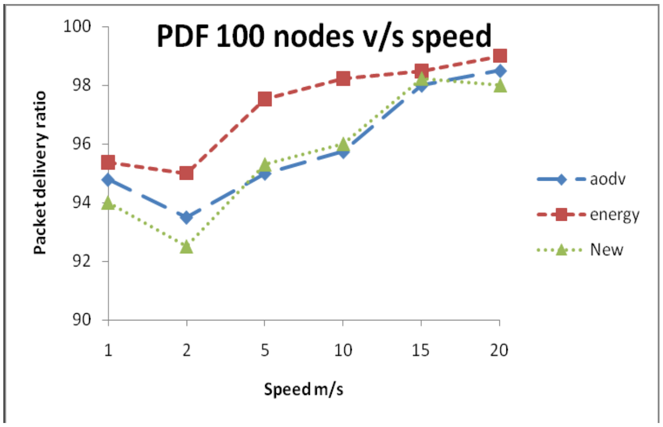

Fig.4: a) Packet delivery ratio for 100 nodes with speed.

Graph 2(a) and 2(b) are packet delivery ratio for 100 nodes with speed and pause time as function respectively. It may be clearly seen that the performance of New is better for denser mediums. Graph 3(a) and 3(b) represents the end to end delay with respect to pause time and speed. Average end-to-end delay is the delay experienced by the successfully delivered packets in reaching their destinations. This is a good metric for comparing protocols and denotes how efficient the underlying routing protocol is, because delay primarily depends on optimality of path chosen. More end to end delay is observed in this case for proposed NEW. The reason is again the more calculation part involved for hash key estimation and checking power status. It should be noted here that only trusted packets are delivered, so some packets does fall because of this reason also. The reduction in packet delivery ratio and increase in end to end delay does not show the ineffectiveness of the proposed scheme. This change will be obvious as more packets are sacrificed to keep them secured and stable. Stability is achieved at the cost of performance. Efforts are on to reduce the margins by reducing the size of Hash key.

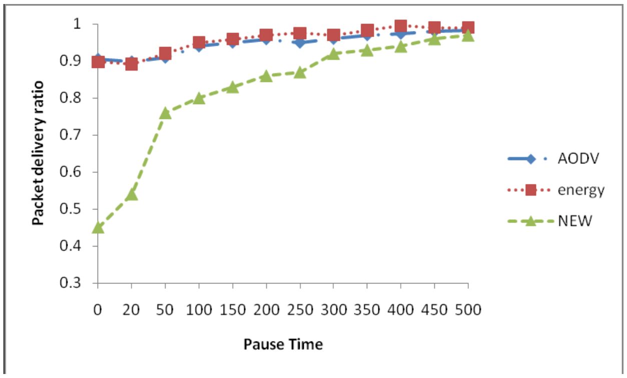

Fig.4: b) Packet delivery ratio versus pause time for 100 nodes

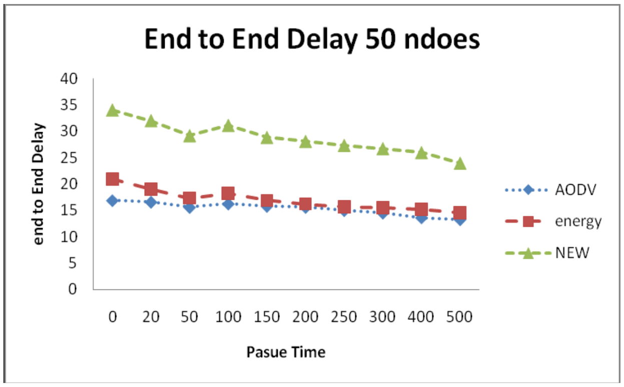

Fig.5: a) End to end delay v/s pause time

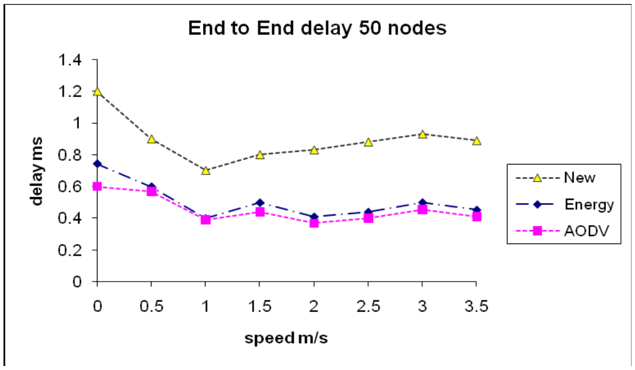

Fig.5: b) End to end delay v/s Speed

6. CONCLUSION

A new scheme has been introduced for secured and power efficient routing for Ad Hoc networks. Scheme has been incorporated on AODV and efforts are on to implement it on DSR as well. Hash Key management has been used as one of the options, though other options can also be considered depending upon need of security. Power status has been taken into account for route selection. The overhead is bound to increase with it, but keeping in view of the better secured and stable routing this is worth it. Proposed scheme is expected to work better in dense environments as selection of path becomes easy in case of link failures. This scheme will be able to take care of external attacks. In order to check internal attacks, some of the techniques that can be used are: Flooding of packets for false route requests, false route replies and also using one way hash to achieve objectives of tampering can be done to take care of internal attacks. Results have been found satisfactory for throughput and mobility patterns as well for the proposed scheme. More study is to be carried out for better throughput and changing mobility patterns. The work is under process to check the proposed scheme under sparse mediums and evaluate results.

7. REFERENCES

[1] T. Karygiannis and L. Owens, ―Wireless Network Security, NIST Special Publication 800-48**,** November 2002.

[2] William Stallings, ―Cryptography and Network Security: Principles and Practice, pages 3–12.Second edition.Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[3] Kush A, Gupta P “*Power Aware Virtual Node Routing Protocol for Ad hoc Networks”* in International Journal of Ubiquitous Computing and Communication (UBICC),Vol. 2 No. 3, pp55-62, South Korea 2007.

[4] C. Parkins and E. Royer, ―Ad Hoc on demand distance vector routing, 2nd IEEE workshop on mobile computing , pages 90-100, 1999.

[5] S. Marti, T. J. Giuli, K. Lai, and M. Baker, ―Mitigating routing misbehavior in mobile ad hoc network, In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking, pages 255–265, 2000

[6] Yonguang Zhang and Wenke Lee, ―Intrusion detection in wireless ad-hoc networks‖, In 6th International Conference on Mobile Computing and Networking (MOBICOM’00), pp. 275– 283, Aug 2000.

[7] B. Dahill, B. N. Levine, E. Royer and C. Shields, ―A secure routing protocol for ad hoc networks, Technical Report UM-CS-2001-037, University of Massachusetts, Department of Computer Science, Aug. 2001.

[8] P. Papadimitratos and Z. J. Haas, ―Secure routing for mobile ad hoc networks, SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), Jan 2002.

[9] Y. C. Hu, A. Perrig and D. Johnson, ―Ariadne: A secure on-demand routing protocol for ad hoc networks, Technical Report TR01-383, Rice University, Dec. 2001.

[10] D. B. Johnson et al., ―The dynamic source routing protocol for mobile ad hoc networks (DSR), Internet Draft, MANET working group, Feb 2002.

[11] A. Perrig, R. Canetti, D. Song, and D. Tygar, ―Efficient and secure source authentication for multicast, In Network and Distributed System Security Symposium (NDSS’01), Feb. 2001.

[12] R. Perlman, ― Fault-tolerant broadcast of routing information, In Computer Networks, n. *7*, pages 395–405, 1983.

[13] L. Zhou and Z. J. Haas, ―Securing ad hoc networks, IEEE Network Magazine, 13(6):24–30, November/December 1999.

[14] S. Marti, T. J. Giuli, K. Lai, and M. Baker, ―Mitigating routing misbehavior in mobile ad hoc networks, In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking, pages 255–265, 2000.Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[15] Singh, S. , Woo, M. , Raghavendra, C. S. (1998), ―Power Aware Routing in Mobile ad hoc networks," *Proc. of the ACM Mobicom 98,* Dallas, October, 1998.

[16] Rodoplu V. and Meng, T. H. (1998), ―Minimum energy mobile wireless networks,"*Proc. of the IEEE International Conference on Communications, ICC'98*, volume 3, pp. 1633-1639, Atlanda, GA, June 1998.

[17] Chang, J.-H. and Tassiulas, L. (2000), Energy conserving routing in wireless ad-hoc networks," *Proc. of the IEEE INFOCOM*, Tel Aviv, Israel, Mar. 2000.

[18] Gupta P. and Kumar, P. R. (1998), ―Critical power for asymptotic connectivity in wireless networks," *Stochastic Analysis, Control, Optimization and Applications: A Volume in Honor of W.H. Fleming*, pp. 547-566, 1998.

[19] Chlamtac, I., Petrioli, C. and Redi, J. (1999), ―Energy conserving access protocols for indentification networks," *IEEE/ACM Transactions on Networking*, 7(1), pp.51-59, Feb. 1999.

[20] Chockalingam, A. and Zorzi, M. (1998), ―Energy efficiency of media access protocols for mobile data networks," *IEEE Transactions on Communications*, 46(11), pp. 1418-1421, Nov. 1998

[21] Chen, B., Jamieson, K., Balakrishnan, H. and Morris, R. (2001), ―Span: An energy efficient coordination protocol for topology maintenance in ad hoc wireless networks," *In 7th Annual Int. Conf. Mobile Computing and Networking 2001*,Rome, Italy, July 2001.

[22] Xu, Y., Heidemann, J. and Estrin, D.(200), ―Adaptive energy-conserving routing for multihop ad hoc networks," Research Report 527 USC/Information Sciences Institute, October 2000.

[23] Lee, Y. Z., Gerla, M., Chen, J., and Caruso, B. Z. A. (2006), ―DFR ("Direction Forward Routing)," *Ad Hoc Sensor Wireless Networks*, 2(2), pp. 01-18, 2006.

[24] Kettaf, N., Abouaissa, A., Vuduong, T. and Lorenz, P. (2006), ―Admission Control enabled On demand Routing (ACOR)," available at draft-kettaf-manet-acor-00.txt, July 2006.

[25] L. Lamport, ―Password Authentication with Insecure Communication‖, Comm. of ACM, 24 (11), pp. 770-772, Nov. 1981

[26] NS Notes and Documentation, available at www.isi.edu/vint pp 15-64.

[27] Kush A., Gupta P. and Hwang C. J. (2008), ―A Hybrid Stable Routing Protocol for Mobile Ad Hoc Networks," *Proc. of the World Wireless Congress" WWC 2008*, San Francisco, USA, pp. 19{25, May, 2008.

[28] Kush A., Hwang, C, ―Proposed Protocol For Hash-Secured Routing Adhoc Networks‖, Masaum Journal Of Computing (MJC)(ISSN 2076-0833) Volume: 1 Issue: 2 Month: September 2009 , pp 221-226.

[29] Kush A., Gupa P,Hwang, C, ―Secured Routing scheme for Adhoc networks‖, IICTE<MAY 2009rnational Journal of Computer Theory and Engineering (IJCTE). May 2009.