IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 11, Issue 1 (May. - Jun. 2013), PP 79-86
www.iosrjournals.org

MDSR to Reduce Link Breakage Routing Overhead in MANET Using PRM

N.Lalitha[1], L Surya Prasanthi Latike[2]

[1] *M.Tech, Assistant Professor,Department of Computer Science & Engineering, Sri Sarathi Institute of Engineering & Technology, Nuzvid, AP,*

[2] *M.Tech, Assistant Professor,Department of Information Technology, Sri Sarathi Institute of Engineering & Technology, Nuzvid, AP,*

Abstract: *Dynamic Source Routing (DSR) algorithm is simple and best suited for high mobility nodes in wireless ad hoc networks. Due to high mobility in ad-hoc network, route may not exit for long time. Hence, DSR algorithm finds an alternative route when the existing communicating route goes down. It becomes a time consuming process if the communicating route fails frequently. In order to avoid this, we propose a modification to the existing DSR protocol named as Modified Dynamic Source Routing (MDSR) Protocol. In this paper, we add a link breakage prediction algorithm to the Dynamic Source Routing (DSR) protocol. The mobile node uses signal power strength from the received packets to predict the link breakage time, and sends a warning to the source node of the packet if the link is soon-to-be-broken. The source node can perform a pro-active route rebuild to avoid disconnection. Intermediate nodes in the route continuously monitor the signal strength at the time of communication, based on a predefined threshold signal value. Intermediate node sends a message to the source node that the route is likely to be disconnected, if signal strength falls below the threshold value. If source receive this message it starts using backup route and if back route also fails then it finds alternative route. The backup route will minimize the time consuming process of finding an alternative route to some extent. Addition of link breakage prediction to DSR can significantly reduce the total number of dropped data packets (by at least 25%). Security to the packets in the MANET is provided by employing a message encryption technique using the concept of deceptive text which ensures confidentiality and authentication to the data.*

KeyWords- *Ad-Hoc Networks, Preemptive, Dynamic Source Routing, Proactive, Deceptive text, Randomized hashing.*

I. INTRODUCTION

There are currently two variations of mobile wireless networks. The first is known as infrastructure network. The bridges for these networks are known as base stations. A mobile unit within these networks connects to and communicates with, the nearest base station that is within its communication radius. As the mobile unit travels out of range of one base station into the range of another, a "handoff" occurs from the old base station to the new, allowing the mobile to be able to continue communication seamlessly throughout the network. Typical applications of this type of network include office wireless local area networks (WLANs). The second type of mobile wireless network is the mobile ad-hoc network or MANET. This type of network needs no base station. Mobile nodes communicate to each other by either directly or through intermediate nodes. Ad-hoc network becomes popular since it can be applied in many situations, such as emergency search-and-rescue operations, classroom, meetings or conference and many more. To facilitate communication within the network, routing protocols used to discover routes between nodes. Routing protocols in MANET, generally, can be categorized as table-driven and on-demand. In table-driven (also called proactive protocol), like in most routing protocol for wired network, each node is required to maintain routing table keep updated whether there is or not a request for routes. In on-demand (also called as reactive protocol), each node seeks for routes only when there is need to do so.

II. DYNAMIC SOURCE ROUTING

The Dynamic Source Routing (DSR) protocol is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. It is based on the concept of source routing, a routing technique in which the sender of the packet determines the complete sequence of the nodes through which to forward the packet. The sender explicitly lists this route in the packet's header, identifying each forwarding "hop" by the address of the next node to which to transmit the packet on its way to the destination host.

The DSR protocol consists of two mechanisms: Route Discovery and Route Maintenance. When a mobile node wants to send a packet to some destination, it first checks its route cache to determine whether it already has a route to the destination. If it has one, it will use this route to send the packet. Otherwise, it will initiate route discovery by broadcasting a route request packet. When receiving a request packet, a node appends its own address to the route record in the route request packet if it did not receive this request message before, and re-broadcasts the query to its neighbors. Alternatively, it will send a reply packet to the source without propagating the query packet further if it can complete the query from its route cache. Furthermore, any node participating in route discovery can learn routes from passing packets and gather this routing information into its route cache.

When sending or forwarding a packet to a destination, Route Maintenance is used to detect if the network topology has changed such that the link used by this packet is broken. Each node along the route, when transmitting the packet to the next hop, is responsible for detecting if its link to the next hop has broken. When the retransmission and acknowledgement mechanism detects that the link is broken, the detecting node returns a Route Error packet to the source of the packet. The node will then search its route cache to find if there is an alternative route to the destination of this packet. If there is one, the node will change the source route in the packet header and send it using this new route. This mechanism is called “salvaging” a packet. When a Route Error packet is received or overheard, the link in error is removed from the local route cache, and all routes which contain this hop must be truncated at that point. The source can then attempt to use any other route to the destination that is already in its route cache, or can invoke Route Discovery again to find a new route.

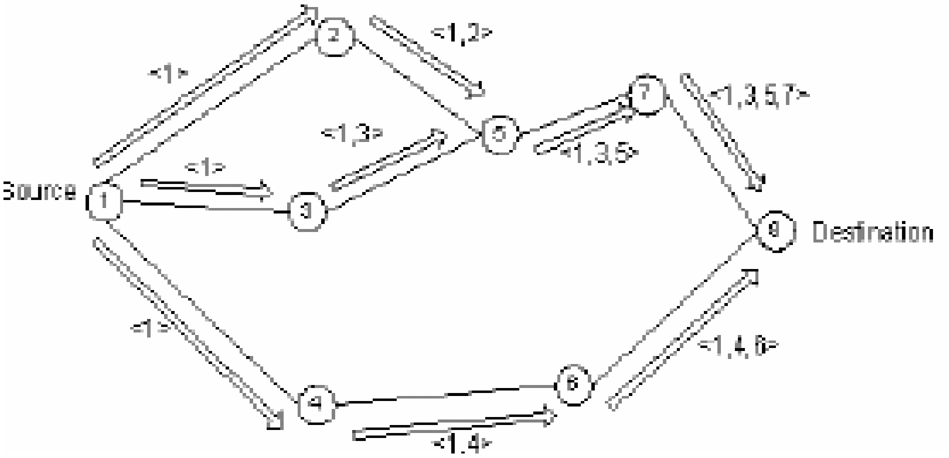


Fig: 1 DSR Route Request

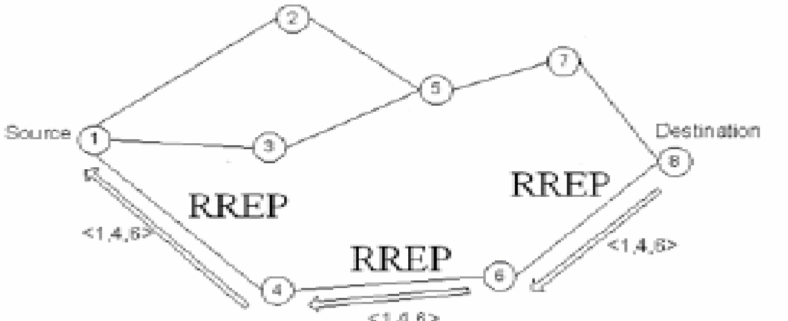


Fig:2 DSR Route Reply

III. Proactive Route Maintenance(Prm)

We assume that all nodes wishing to communicate with other nodes within the ad hoc network are willing to participate fully in the protocols of the network. Each node participating in the network should also be willing to forward packets for other nodes in the network. We refer to the minimum number of hops necessary for a packet to reach from source to destination. We assume that he diameter of an ad-hoc network will be small(5 to 10 hops), but greater than 1. Packets may be lost or corrupted in transmission on the ad-hoc wireless network. A node receiving a corrupted packet can detect the error and discard the packet. The GPS and signal strength methods both use physically measured parameters to predict the link status. The node with GPS can know the position of itself directly. But GPS currently is not a standard component of mobile devices and in the metropolitan area and indoor, the signal can be too weak to be received. The signal strength method only consumes receiving node’s computing power, and does not depend on any additional device. It is used in this paper. At first we assume that the sender power level is constant. Received signal power samples are measured from packets received from the sender. From this information it is possible to compute the rate of change for a particular neighbor’s signal power level. Because the signal power threshold for the wireless network interface is fixed, the time when the power level drops below the acceptable value can be computed. Characteristics of

PRM include: Freshness. All nodes near an active route have the up-to-date routing information. Broken paths are eliminated, new paths recognized, and non-optimal paths replaced by optimal ones.
Robustness: An active node that is forwarding data packets usually maintains several fresh alternative paths. After one path fails, the data packet is usually forwarded via another path without causing packet loss or extra delay. PRM will resort to a route discovery operation only after all alternative paths have failed.
Lightweight maintenance: Unlike in existing proactive routing protocols, the route maintenance is confined to those small areas surrounding active routes, where control packets make only a small portion of data transmission. As the lifetime of a route is lengthened, the overhead of the proactive route maintenance can be compensated by the less frequent route discovery operations. The proposed Concept is illustrated using the following example.

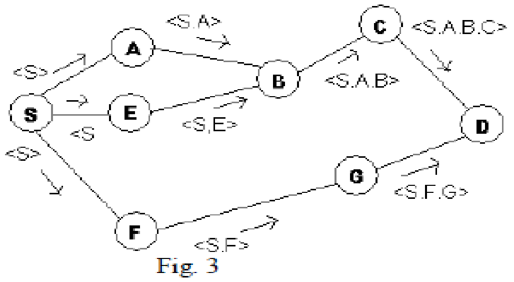
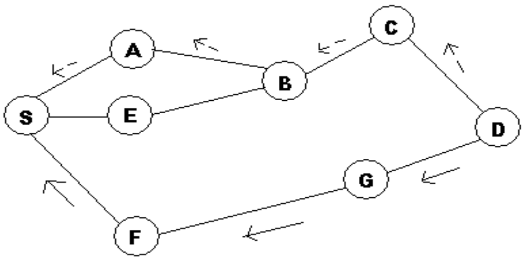


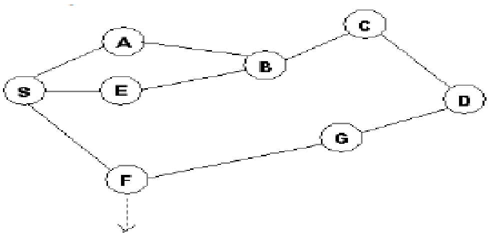
Fig. 3

When a source node S want to send message to the destination node D, it initiates route discovery by broadcasting the RREQ packet to its neighbors (A, E, F) as shown in Fig 3. The intermediate nodes (A, E, F) on receive the RREQ packet rebroadcast the packet to its neighbors by appending its id in the route record of the RREQ packet. Similarly, other intermediate nodes also forward the RREQ packet to the destination. When the destination node D receives two or more RREQ packets from the same source through different routes, it finds the two best routes based on the no of hopes. The route, which has least number of hopes. The route which has least number of hops it becomes primary<S, F, G>, and second least number of hops route becomes backup route<S, A, B, C>. The destination node D sends Route Reply (RREP) packet using the Primary (<S, F, G>) and Backup(<S, A, B, C>) route as shown in the following Fig. Each RREP packet contains the Primary as well as the Backup route information. When source node S receives first RREP packet form destination, it treats this is the primary route and wireless communication is more error prone compared to wired network. To improve the reliability we are sending route reply (primary + backup routes information) through the primary and the secondary route. If any one packet gets corrupted at the time of transmission, source must be able to use the other packet.



Primary Route → <S.F.G> + {<S.A.B.C>}}
Backup Route ⇢ {<S.A.B.C> + {<S.F.G>}}

The communication between the source node S and destination node D commence using the primary path<S, F, G>. During communication, the node F starts moving away from S. When the signal strength of node F falls below threshold T, it sends a warning message "Path likely to be disconnect" to source node S. As soon as S receives the warning message, it starts using the Backup route along with primary route. Whenever destination node receives the data packets from the source node through two different paths (Primary + Backup), it sends acknowledgement through both the paths. If source node S receives an acknowledgement from the destination node through the Backup route, it makes preemptive switch over to the Backup route; otherwise S initiates the route discovery process.



A. Generating the Warning Message based on the Signal Strength

Let us consider the following scenario while using the Backup route.

Case 1: Node C is moving toward node G, as shown in Fig 4

As node C is moving towards node G, the signal strength increases and Backup route become more stable.

Case 2: Node C is moving away from node G, as shown in
Fig 5.

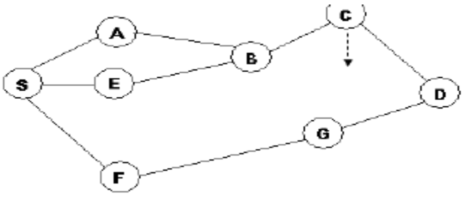


Fig. 4

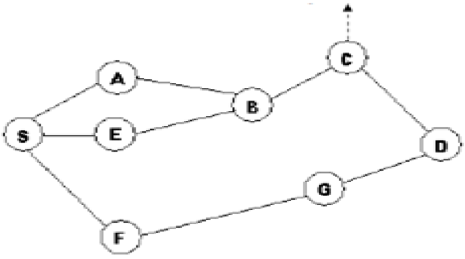


Fig.5

As node C is moving away from node G, the signal strength of C falls below the threshold T and as a result the Backup route fails. Let p($0 \leq p \leq 1$) is the probability of the route failure in case of DSR. In the best-case p=0 and in the worst case p=1. Hence on an average case the probability of route failure p=0.5 (50%). Similarly in the proposed Proactive routing in Dynamic Source Routing Protocol for Wireless Ad-hoc Networks with Backup Route.

The probability of Primary route failure is p=0.5 (50%) ----(1)

The probability of backup route failure is p=0.5 (50%) ---- (2)

Form (1) and (2) we conclude that the probability of both the route failure p=0.25 (25%). Therefore, Modified Dynamic Source Routing Protocol for Wireless Ad-Hoc Networks with Backup Route has a significant effect on the performance as it improves the reliability form 50% to 75% with minimal control overhead. The threshold value plays an important role for control packet overhead.

Case 1: If threshold T is large: It may send false warning to source node to use backup route.

Case 2: If threshold T is small: Source node may not get sufficient time to discover new route, if backup route fails. Therefore threshold T value is set moderate, to overcome above-mentioned drawbacks. A Preemptive region is defined around every node as shown in the figure 6 for node A. As soon as node C enters the preemptive region, a warning message is sent to the sender node A. Then the node A initiates a route discovery process. With the establishment of a new route, data transmission is continued along this new route. The time required to discover a new path can be termed as recovery time Trec. Hence the time between the warning and the path break Twarn should be atleast or slightly greater than Trec.

In order to determine the optimal range, it is necessary to exchange the location and velocity information of the nodes amongst all the nodes depending on the receiver signal power. The receiver signal power, Pr = P0 / rn at a distance r from the transmitter, where P0 is the transmitted power and path loss exponent n is typically between 2 and 4. The minimum power receivable by the device is the power at the maximum transmission range,

Pd = P0 / d4

Similarly, the preemptive signal power threshold is the signal power at the edge of the preemptive region. In addition, for a preemptive region of width of w, the signal power threshold is

Psafe = P0 / d4 safe

Where dsafe is equal to (d- *w*) and *w*=relative speed*Twarn The preemptive ratio α is defined as

α =Psafe / Pd = range/ (range- w).

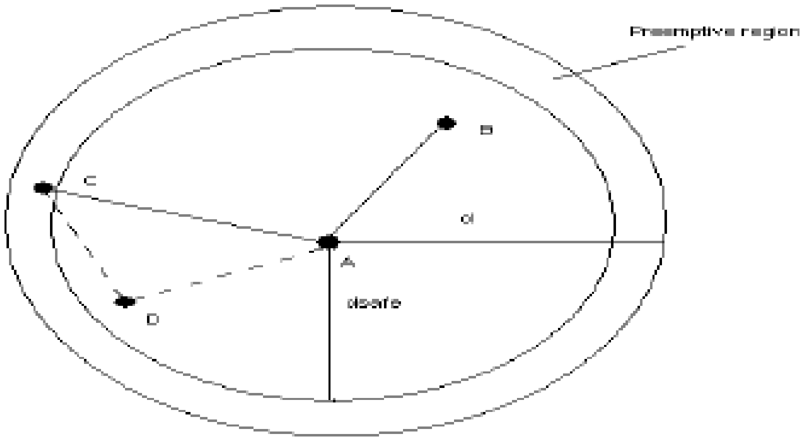


Fig: 6 Preemptive Region

In reality, the received signal power may experience sudden fluctuations due to channel fading and multipath effects, which will trigger a false warning, causing unnecessary route request floods. This may result in lower quality routes being initiated and also increasing the routing overheads. In cellular networks, an exponential average of the signal power is used to verify that the signal power drop was not due to fading. However, if the traffic is bursty or infrequent, the preemptive region may be fully crossed by the time enough packets are received to drop the average below the threshold. Therefore quicker power estimates can be achieved by sending a warning whenever the instantaneous power drops below the threshold and checking the warning packet received power when it is received by the source. If the warning packet power is also below the threshold, there is a good probability that the warning is real.

B. Generating the Warning Message based on 'Age of the Path'

With transmissions being done along the same path, relay nodes will experience a continuous drain of their battery power for the same source destination pair, which may result in path failure. Therefore alternate route discoveries are required before the onset of failure. Nodes keep a record of their most recent encounter times with all other nodes. With a path discovery being made, the source node sets a timer. The preemptive warning is generated based on two parameters- Age of the path defined as the time difference age between the transmissions of two consecutive route discovery packets from the source to the same destination and threshold value Γ is defined for the age of the path. As long as age is lesser than Γ, data transmission can be continued on the same path. When the timer value exceeds the threshold Γ, a warning message is generated leading to a new path discovery. However, this new path may or may not be the shortest path to the destination. The choice of the threshold depends on node density of the network. If the node density is small with lesser number of paths available, Γ must be large.

IV. MESSAGE ENCRYPTION USING DECEPTIVE TEXT

The data packets sent to the intended receiver were encrypted by using the proposed concept of Deceptive Text. In this paper we propose that, deceptive text instead of encrypted plaintext is sent to receiver. The deceptive text can be in any form of text which is constructed by ASCII code. The deceptive text can have no relation with the original plaintext.

In this scheme we used a Character Position Table (CPT), which contains positions of each character in the deceptive text. From the CPT we generate Plaintext Index File (PIF), which is a series of character positions taken from CPT that correspond to the characters in the plaintext. Finally we encrypt the Plaintext Index File (PIF) and send it to the receiver. Therefore, the real data we send is the deceptive text and the encrypted index file.

At the receiver the PIF is decrypted and the CPT is generated from the cheating text. The plaintext is generated by indexing PIF into the CPT. In this scheme we have used digital signature to provide authentication for the receiver about the Deceptive text.

A.Generating Digital Signature

When using digital signature algorithms to generate a digital signature for a message, the message must first be processed using one of the approved hashing algorithms. We apply the randomization to the message prior to hashing.

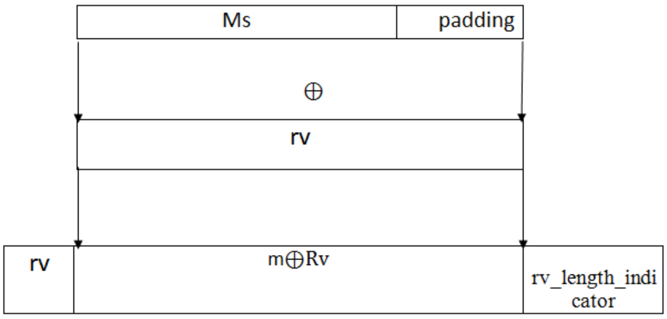


Fig 7: Process of randomizing a message

B.Encryption Process

Algorithm:-
Input:-Plain Text, Deceptive Text.
Procedure:-
1. Verify whether character's kinds in deceptive text satisfy character's kinds in plain text. If satisfied, goto step2.If not, discard the current deceptive text and generate new one.
2. Generate Character Position Table (CPT) from the deceptive text.
3. Generate Plaintext Index File (PIF) using CPT.
4. Randomize deceptive text using a random value (rv).
5. Generate digital signature (DS) of randomized deceptive text using MD5 algorithm.
6. Encrypt PIF and rv using AES.
7. Send deceptive text, encrypted PIF, encrypted rv, and digital signature (DS).

C.Decryption Process

Algorithm:-
Input:-Digital signature (DS), Encrypted Random value (rv), Deceptive Text (DT), Encrypted Plaintext Index File (PIF).
Output:-Plaintext.
Procedure:-
1. Decrypt Random value (rv) using symmetric AES.
2. Randomize Deceptive Text (DT) using Random value (rv).
3. Generate digital signature (DS1) of randomized deceptive text.
4. Verify whether received digital signature (DS1) are DS are equal. If equal goto step5.If not, discard received DS.
5. Decrypt PIF using symmetric AES algorithm.
6. Generate Character Position Table (CPT) from deceptive text and recover plaintext by indexing PIF into CPT.

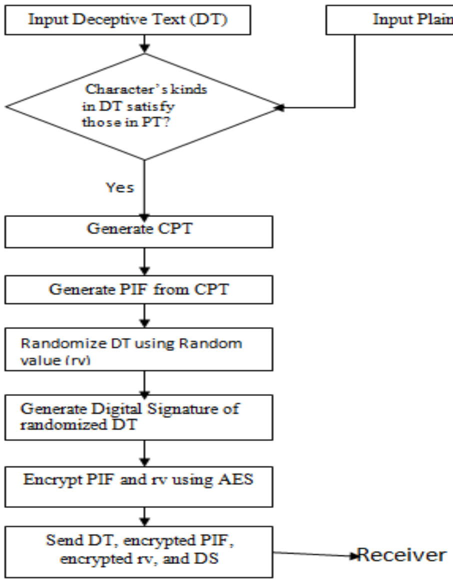

Input Deceptive Text (DT)
Input Plain Text (PT)
Character's kinds in DT satisfy those in PT?
Yes
Generate CPT
Generate PIF from CPT
Randomize DT using Random value (rv)
Generate Digital Signature of randomized DT
Encrypt PIF and rv using AES
Send DT, encrypted PIF, encrypted rv, and DS
Receiver

Fig 8: Process of Encryption

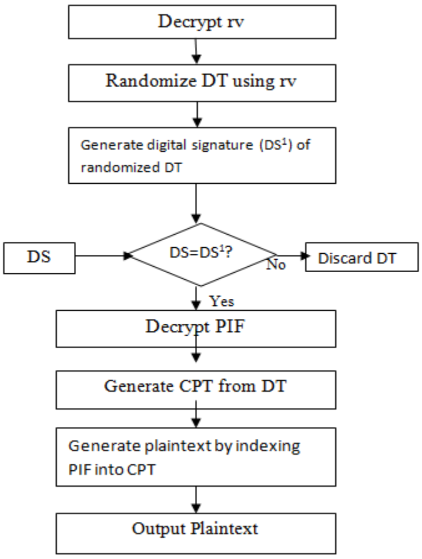


Fig 9: Process of Decryption

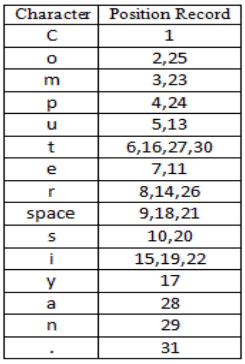
D.Example

We assume that

Plaintext: cat is my pet.

Cheating text: computer security is important.

According to the cheating text, we generate the CPT as follows:



Character	Position Record
c	1
o	2,25
m	3,23
p	4,24
u	5,13
t	6,16,27,30
e	7,11
r	8,14,26
space	9,18,21
s	10,20
i	15,19,22
y	17
a	28
n	29
.	31

Fig 10: Character Position Table

Then we compare each character in plaintext with CPT’s characters and randomly chose a position record to make the PIF.The PIF is: 1 28 16 21 15 20 18 3 17 9 24 7 6 31

V. CONCLUSION

DSR with PRM mechanism detects early about the link that is likely to break soon, and hence it uses a backup path before the existing link fails. This paper explains the preemption of Primary to Backup route by the source node S, whenever the signal strength of the primary route falls below the threshold value T. The modified DSR will improve the communication reliability between the source and destination node even if the mobility is high. In addition, the link breakage prediction in DSR can significantly reduce the total number of dropped data packets (by at least 25%). Also security to the packets in the MANET is provided by employing a message encryption technique using the concept randomized hashing method.Finally, it provides a high-level of protection for the data at low computational complexity.

REFERENCES

[1] Hongbo Zhou, “A Survey on Routing Protocols in MANETs,” Technical. Note March 2003.

[2] Siva Ram Murthy, B.S, Manoj, “Routing Protocols for Ad Hoc wireless Networks,” in Ad Hoc wireless networks: Architectures and Protocols, Chapter 7. Pearson Publication.

[3] T. Goff, N.B. Abu-Ghazaleh, D.S. Phatak and R. Kahvecioglu, “Preemptive Maintenance Routing in Ad Hoc Networks”, journal of parallel and Distributed Computing, Special Issue on Wireless Mobile Communication and Computing 2003.

[4] Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park, “A Performance Simulation for Route Maintenance in Wireless Ad Hoc Networks”, ACM,2004

[5] William Stallings,”Network Security Essentials”.

[6] Quynh Dang,”Randomized Hashing for Digital Signatures”.

[7] Chu-Hsing Lin and Tien-Chi Lee,”A Confused Document Encryption Scheme and Its Implementation”.

[8] C. E. Perkins and P. Bhagwat. Highly dynamic destination sequenced distance vector routing (DSDV) for mobile computers, In ACM SIGCOMM, pages 234-244, 1994.

[9] X. Hong, T. Kwon, M. Gerla, D. Gu and G. Pei.A Mobility Framework for Ad Hoc Wireless Networks. In Proceedings of ACM Second International Conference on Mobile Data Management (MDM ’2001), Hong Kong, Jan. 2001.

[10] A Group Mobility Model for Ad Hoc Wireless Networks X. Hong, M. Gerla, G. Pei, and C.-C. Chiang. In Proceedings of ACM/IEEE MSWiM’99, Seattle, WA, Aug. 1999.

[11] A. Montresor, H. Meling, and O. Babaoglu, “Load-balancing through a swarm of autonomous agents,” inProc. 1st Workshop Agent Peer-to-Peer Syst., 2002, pp. 125–137.

[12] G. W. Flake, The Computational Beauty of Nature. Cambridge, MA: MIT Press, 2000.

[13] R. Sutton and A. Barto, Reinforcement Learning. Cambridge, MA: MIT Press, 1998.

[14] L. Kaelbling, M. Littman, and A. Moore, “Reinforcement learning: A survey,” J. Artif. Intell. Res., vol. 4, pp. 237–285, 1996.

[15] C. Watkins, “Learning from delayed rewards,”Ph.D. dissertation, King’s College, Cambridge, U.K., 1989.

[16] A. Moore and C. Atkeson, “Prioritized sweeping: Reinforcement learning with less data and less time,” Mach. Learning, vol. 13, pp. 103–130, 1993.

[17] K. Doya, K. Samejima, K. Katagiri, and K. Kawato, “Multiple model-based reinforcement learning,” Neural Comput., vol. 14, no. 6, pp. 1347–1369, 2002.

[18] D. Johnson, D. Maltz, and J. Broch, “DSR: The dynamic source routing protocol for multihop wireless ad hoc networks,” in Ad Hoc Networking. Reading, MA: Addison-Wesley, 2001, pp. 139–172.