International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 06, June-2018

Detection of Packet Dropping in Adhoc Network

Hina Khan[1]
PG Scholar,
Department of Computer Science & Engineering
Sr Group of Institutions
Lucknow, Uttar Pradesh (India)

Kamal Soni[2]
Assistant Professor
Department of Computer Science & Engineering
School of Management Sciences
Lucknow, Uttar Pradesh (India)

Mohini Singh[3]
PG Scholar,
Department of Computer Science & Engineering
Sr Group of Institutions
Lucknow, Uttar Pradesh (India)

Santosh Kumar Singh[4]
Assistant Professor
Department of Computer Science & Engineering
School of Management Sciences
Lucknow, Uttar Pradesh (India)

Abstract **- Mobile Ad hoc Network (MANET) is self-configuring network of mobile node connected by wireless links and considered as network without infrastructure. Routing protocol plays a crucial role for effective communication between mobile nodes and operates on the basic assumption that nodes are fully cooperative. Because of open structure and limited battery-based energy some nodes (i.e. selfish or malicious) may not cooperate correctly. After becoming part of active path, theses nodes start refusing to forward or drop data packets thereby degrades the performance of network. In this paper, a new reputation based approach is proposed that deals with such routing misbehavior and consists of detection and isolation of misbehaving nodes. Proposed approach can be integrated on top of any source routing protocol and based on packets and counting the number of data packets that are dropped in the communication. The trace file that is generated after the encryption decryption procedure have the exact values of the packet drop in that efficient routing. The trace file have the drop time and the node that is responsible for packet dropping .Detecting the packet drop is the main goal of Research.**

RELATED WORK

A. MANET and its Architecture

The ability to establish communication without an infrastructure and the capacity to communicatebeyond the node's wireless transmission range embarks Mobile Ad hoc Networks (MANET) as the deployment ground for various fields such as wireless sensor networks, ubiquitous networks and peer-to-peer networks. Implicitly, the low cost, undemanding maintenance and simplicity acknowledges mobile wireless networks as an alternative to the existing wired networks. The proliferation of communication devices and the evolution of technology confirm that it is the tool, which can turn the existing computing space into smart space.

Though MANET promises to be the operational base for most of applications, security issues are paramount in such networks even more so than in wired networks. The fundamental problem in mobile ad hoc networks is the lack of consistency to deliver information to the intended node. At the same time, the need to address the availability of services irrespective of the mobility creates serious challenges in the design.

B. ATTACKS IN MANET AND SECURITY EVALUATION

Securing wireless ad-hoc networks is a highly challenging issue. Security of communication in WSN is important for secure transmission of information. Absence of any central coordination mechanism and shared wireless medium makes WSN more vulnerable to digital/cyber-attacks than wired network there are a number of attacks that affect WSN. Different possible attacks on the flow of data and control information can be categorized as follows: [1][2][3][4][5]

- Spoofed, altered, or replayed routing information
- Selective forwarding attack
- Sybil attack
- Black hole attack
- Wormholes attack

B. MALLACIOUS NODE MITIGATION IN MANET

Malicious node mitigation can be classified into two categories: [6][7][8][9]

(i) prevention and protection,

(ii) detection and response.

A prevention mechanism guards against a malicious node's attack by applying cryptographic mechanisms such as encryption and authentication. However, it cannot guard against insider attacks. A detection and response mechanism detects misbehavior activities and responds to an attack .In this dissertation, the main focus is on addressing detection of packet drop in the mobile adhoc network using cryptography.

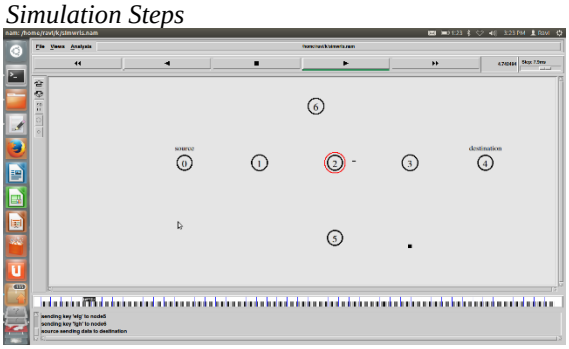
International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 06, June-2018

C. *PROPOSED SOLUTION: RSA CRYPTOGRAPHIC ALGORITH TECHNIQUE*

Proposed Solution simulation is based on the approach to detect the packet drop algorithm using the encryption and decryption algorithm. For the implementation or simulation of the exact scenario network simulator 2 on the Linux 13.10 version has been used .Simulation work is based on the network simulator 2 .There are some parameters that are to be set to implement the packet drop attack using encryption and decryption technique in the simulation . Different tools and simulators used are:[10][11][12]

- NS2: (Network Simulator version2)
- C++
- OTCL

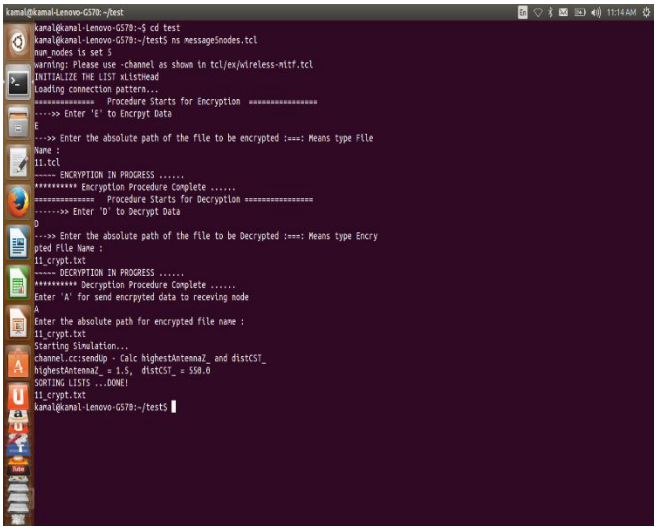
D. *Simulation Steps*



Detection of Packet Drops.

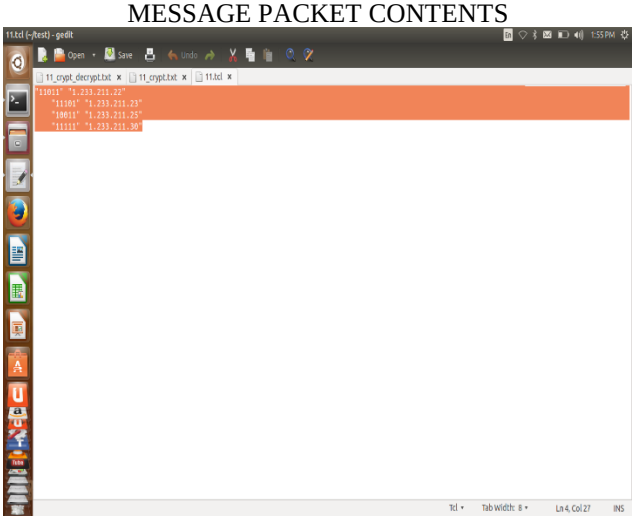
Above figure shows how the packets are dropping and which node is responsible for packet drop. We can visually see the node 3 is dropping the packet but the time of dropping the packet can only be calculated after the trace file is generated in further steps.

EXECUTING COMMANDS FOR ENCRYPTION AND DECRYPTION



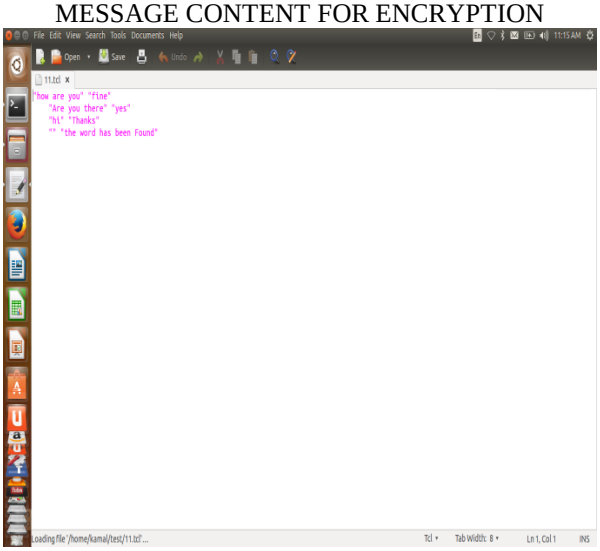
Linux console will be used to simulate the process. Above diagram shows the console is listing the command executed. This calls encryption and decryption process and will send the encrypted message to the receiving node .

MESSAGE PACKET CONTENTS

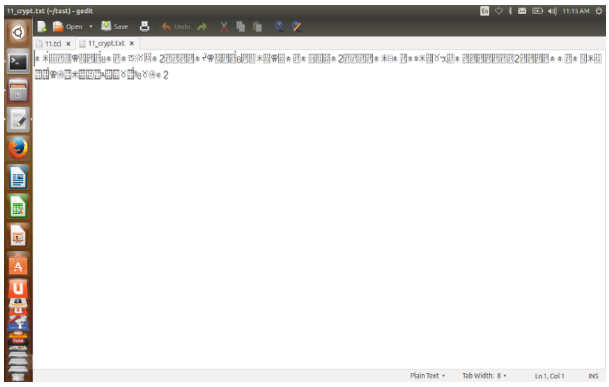


In this snapshot it will showing the keys that are used for encryption. tcl contains keys and ip address is the scripting language that is used to create a file.

MESSAGE CONTENT FOR ENCRYPTION



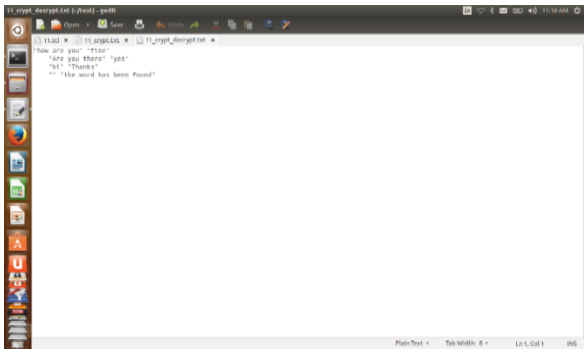
ENCRYPTED MESSAGE PACKET CONTENT



In above file message is encrypted using RSA algorithm and the file is containing the encrypted message that is showing in the snapshot the encrypted file is generated after completing the encryption process that is simulated in NS2.

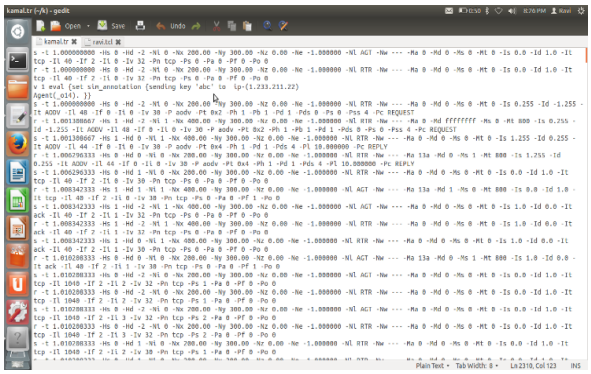
International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 06, June-2018

DECRYPTED MESSAGE PACKET CONTENT



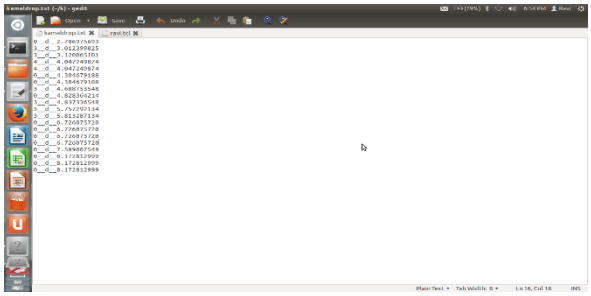
In this file the decrypted message is showing, this message is exactly the same message that was sent for encryption .The encrypted message is showing in the earlier snapshot. In this snapshot the message is decrypted and showing in this snapshot.

AUTOGENERATED TRACE FILE



This is trace file named kamal.tr. It is generated after process is complete. It exactly shows which node is receiving the packet and which node is dropping or sending the packet.

AUTOGENRATED TRACE FILE FOR DROP PACKETS



This snapshots state that only drop of the packet that d denotes the drop of the packet and node which is dropping the packet and the time is shown here that at which time packet is dropped from the particular node.

PROPOSED ALGORITHM

after a root discovery
arrange all nodes in asending order in node[n]
node[source] will generate random list of keys and keep it with itself in array key[n-1]
for i=1 to n-1 i++
do
send(key[i]) to node[i] from node[source]
endfor
data transmission start from source to receiver node.
after each Threshold time t the receiver will receive a data packet
foreach node in node[n] starting i=1 to n-1
do
set receiver=node[i]
if(input Buff[receiver]==is Empty)
do
search for alternate root to node[source]
if root exists
send encrypt request message using key[node[receiver]]
to node[source]
break;
else
set receiver =parent[parent[receiver]]
if parent[parent[receiver] not exist]
then set receiver= parent[receiver]
now send encrypted request message to node[source] via receiver
end if
end for
if buff[node[source]] received encrypted message
do
start decryption using key[node[i]]
if(Packet contains request message)
makelist defaultnode[emptyplace] =node[i-1]
endif
end if
print [defaultnode]

In this proposed algorithm first it will send the keys to the destination to each and every node
Alongwith the message .After that when the packet transmission starts the packet drop happens eventally and the trace file is generated. In that trace file we have the values of total drop packets and total time is also estimated through the trace file alongwith time stamp. When the packet drop occur at any node or if any node rejects the packets received and does not forward it further then for the threshold time the next node after the packet dropping node will wait and then it will generate the request message and encrypt it by using its own key provided by the source node at the time of root discovery and then via alternate path it will send this encrypted message to the source node and source node can only decrypt it because only source node has the list of all keys that it would provide to all nodes in the beginning of the algorithm. And find out the node that send this encrypted message and possibly the parent node of request sender node is defaulter and that is kept in the default node list.

E. RESULT ANALYSIS

In this study, the focus is on the packet dropping attack and the corresponding detection mechanisms mentioned above. The assumption here is that malicious nodes participate in routing information exchange or otherwise act so as for it to be possible that they are selected as intermediate nodes along routes from source nodes to destination nodes.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 06, June-2018

However, they will drop all data packets that they are supposed to forward. The watchdog and cop mechanisms are studied in this chapter to mitigate the attack using packet delivery ratio (throughput) as the performance metric.

General Analysis

This chapter presents a simple analysis of Packet Delivery Ratio (PDR) in ad hoc net-works with and without malicious nodes and with different detection mechanisms. We define PDR as follows.[13][14]

$$PDR = \frac{\text{Total number of received packets at destination}}{\text{Total number of sent packets by source}}$$

In order to simplify our analysis, we make some assumptions:

One source and one destination are considered in a grid network (single flow).

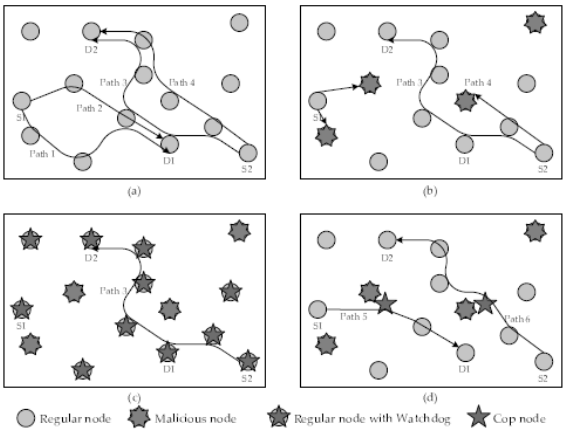
Malicious nodes perform a 100% data packet dropping attack.

Since the packet dropping attack is studied, the same assumptions as described previously hold. A malicious node participates in routing information exchange but drops all data packets. Therefore, a destination will not receive any data packets if a malicious node is an intermediate node along a selected path and the PDR is zero since the total number of received packets is zero.

The performance depends on the probability of choosing a path to the destination. When a malicious node is selected as an intermediate node, the PDR is zero (as described above). In contrast, when a path contains only regular nodes, all packets will be received at a destination and the PDR is one since total number of received packets equals to total number of sent packets (note that we assume that there is no congestion or other packet losses here).

The total number of paths with a given routing metric from a source to a destination has to be known in order to calculate the probability of choosing a path that contains a malicious node or one that has only regular nodes. When a malicious node is detected and excluded from the network, the number of paths is changed and a new probability has to be recalculated. This process is recursively continued until the last malicious node is detected. There are n stages to be considered for n malicious nodes as described next.

The average PDR can be computed using a probability weighted average of the number of received packets at a destination for all possible cases. In our analysis, a constant bit rate traffic is assumed and packets start sending at time 0. Therefore, the number of sent packets is constant for the observation duration. To analyze the average PDR performance, parameters are defined as follows.



Let:

N = Set of non-detected malicious nodes

M = Set of all malicious nodes

n = Total number omalicious nodes mi= A malicious node i

Ej= Event that j malicious node(s) is (are) already detected

T = Total observation time in seconds

R = Data rate in packets per second

Tdeti= Detection time when theithmalicious node is detected

With watchdog mechanism, the average PDR is shown here

PDRAVG = P{choose path excluding nodes in M}× PDR{choose path excluding nodes in M}

$$+\sum_{i=1}^{n}\{\text{choose path including node mi}\}\times PDR\{\text{choose path including node mi}\}$$

where, PDR(choose path including node mi) is the PDR of choosing the node mi in the path but there are other paths, that can be chosen after mi is detected at the time Tdeti . In what follows, we use a shorter notation. P(choose path excluding nodes in M) is written asP (not choose M), P (choose path including node mi)is written as P (choose mi) and so on. Moreover,After a malicious node is detected, that node is excluded from all the paths from a source to a destination. nodes. The total number of sent packets is RT and the total number of received packets, after the last malicious node is detected, is R(T¡Tdetn). Hence the PDR is the ratio of these two quantities. This is a simple analysis that assumes that malicious nodes are detected sequentially, one by one, and multiple malicious nodes are not present along the same path. The analysis becomes more complicated otherwise. Whenn malicious nodes are in the network, the total number of possible cases to be considered is:The intuition behind this equation is as follows. The PDRavg is recursively computed when a malicious node is detected until all malicious nodes are detected. This implies n! because we assume that any one of the n malicious nodes may be detected first. While this is not really true because the malicious node that is detected first depends on the path selected and detection mechanism, our assumptions limiting traffic to one flow and one malicious node per path allows this approximation. Every time a malicious node is detected, one case, where no malicious node is chosen, For example in a static network with 3 malicious nodes, the total number of cases is 16, which comes from 2 parts: the probability of

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 06, June-2018

choosing any one of the malicious nodes and the probability of not choosing a malicious node. For the first part, there are 3 stages for this example and each stage depends on the number of malicious node left to be detected. The first stage has 3 malicious nodes to be detected and the second stage has 2 malicious nodes to be detected and the last stage has 1 malicious node to be detected. The total number of cases for choosing any malicious nodes is 3,2,1 for all 3 stages. The second part is the cases for not choosing any malicious nodes. The first stage has 1 possible case, the second stage has 3 possible cases and the last stage has 6 possible cases. Total number of cases of not choosing any malicious nodes is 1+3+6. Therefore, the total number of cases for this example is 16 cases.

Since the cop mechanism uses an algorithm similar to that of the watchdog mechanism, the differences between the two mechanisms arises due to the fact that the only detecting nodes are cop nodes. The cop node has to be in the transmission range of a forwarding node and the intended receiver to correctly detect a malicious node. If a cop node is moving in a network (mobile cop), it has a limited time to monitor each node's activity. If it is static, called a static cop, its performance is similar to the watchdog mechanism, but it may have limited coverage. Therefore, the cop mechanism usually takes equal or longer detection time than the watchdog mechanism. The PDR calculation is similar to the watchdog mechanism but the difference is in the detection time.

PROPOSED MODEL RESULT ANALYSIS

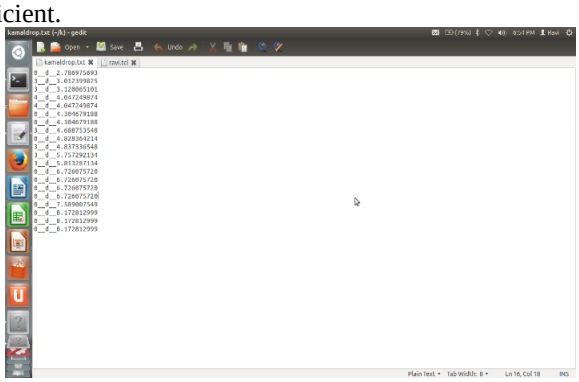
The result what we get in the simulation is depends upon the packet drop in the given network the packet drop calculated from the trace file that is auto generated after the simulation. The trace file is responsible for detecting the node and the network from where the packet drop anomaly occurs. The file is responsible to detect whether the network node is a sender or receiver. We have simulated the model in small network in the local machine. The ad hoc network consists of 5 nodes. The receiver nodes unicasts the encrypted message to the corresponding nodes in the preselected route. The message is then carried forward in the similar manner till it reaches the receiver node. In case the preselected route is faulty and there is a scenario of intermittent packet drop. The trace file is auto generated by the system to automatically detect the number of packet drops that have occurred in a specific node. The trace file records all the packet drops and the respective nodes in which the packet drop occurs.

The detection method would be responsible to automatically notify the route discovery engine to process and analyze a new route if the number of packet drops is intolerable.

The exact node that is dropping the packet = 0,3,4

The time estimated in the packet dropping = 15ms.

In our scenario the exact packet drop or loss is 20 and we also detected that at which time they are dropping the packet and they also detected the total time taken in the process is 15ms. In there they are investigating only limited number of packets and in our scenario the natural packet dropping is detected and the whole dropped packets are detected and the exact node that is dropping the packet is detected so in proposed idea the packet dropping is detected on the particular node and in their proposed idea they are node identify the particular node so my approach is more efficient.



Detection Packet Drop And Time

In this snapshot first row is stated as nodes that are dropping the packet and the second line stated as the time. This time is stated when the exact packet is dropping the packet.

We found that the RSA algorithm used for encrypting the text performs efficiently. RSA algorithm is used to generate public key and private key. The public and private key is different for all nodes in the entire network. Public key is used for encryption and Private key is used for Decryption. Source node send request to receiver after receiving the request destination node send the request to trust authority (TA) with the secret message. Our main aim is to detect the packet drop in this scenario I have just used this scenario on the efficient channel of the network.

I am using RSA algorithm for encryption and decryption because it will allow me to implement my idea of cryptography. The RSA algorithm is the backbone of this research drop attack like acknowledgement based and many other like watchdog algorithm. Wireless effects impact the performance of not only the packet dropping attack but also the detection mechanisms. When the overall transmission range is increased, the effect of the attack is reduced and the detection mechanisms can detect a malicious node easier since it can overhear most of the communications in the network.

This study shows how to detect the packet drop in the efficient scenario of the network .the proposed idea is most efficient one because it will calculate the packet drop and the time of the packet drop and the nodes that are dropping the packet in the given scenario. The process that is used for detecting the packet dropping is the encryption and decryption, because it will drop the packets and the packets that are contain the message are dropping by some of the node that is participating in the transmission communication.

The related future work is to be on the studies of more and maximum efficient path that can involve most of the ad hoc nodes that are participating in the network .In future we can implement it on the bigger scale for 100 to 200 nodes . In this process we to make this mechanism more powerful and more authenticate to detect the packet drop on the bigger scale the encrypted data can be sent widely by any of the network so it can properly detect the packet drop in 200 or maximum nodes.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 06, June-2018

REFRENCES

[1] Y.-C. Hu, A. Perrig, and D. B. Johnson, \Rushing attacks and defense in wireless ad hoc network routing protocols," in Proceedings of the 2003 ACM Workshop on Wireless Security (WiSe 2003). ACM, September 2003, pp. 30-40.

[2] Y. an Huang and W. Lee, \Attack analysis and detection for ad hoc routing protocols," in Proceedings of The 7th International Symposium on Recent Advances in IntrusionDetection (RAID 2004), September 2004.

[3] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, \Mitigating byzantine attacks in ad hoc wireless networks," Center for Networking and Distributed Systems , Johns Hopkins University," Technical Report, 2004.

[4] D. Spiewak, T. Engel, and V. Fusenig, \Towards a threat model for mobile ad-hoc networks," in ISP'06: Proceedings of the 5th WSEAS International Conference on In-formation Security and Privacy. Stevens Point, Wisconsin, USA: World Scienti¯candEngineering Academy and Society (WSEAS), 2006, pp. 35-40.

[5] I. F. Akyildiz, X. Wang, and W. Wang, \Wireless mesh networks: A survey," ComputerNetworks Journal (Elsevier), vol. 47, no. 6, pp. 445{487, March 2005.
MANET Working Group, INTERNET-DRAFT, July 2004, expiration: January 2005. [Online]. Available: http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-10.txt

[6] A. Perrig, R. Canetti, D. Song, and J. Tygar, \The tesla broadcast authentication protocol," in CryptoBytes, 2002, pp. 2-13.

[7] Y.-H. Hu, A. Perrig, and D. Johnson, \Ariadne: A secure on-demand routing protocolfor ad hoc networks," in The 8th Annual International Conference on Mobile Computing and Networking, 2002.

[8] Y.-C. Hu, D. Johnson, and A. Perrig, \Secure efficient distance vector routing in mobilewireless ad hoc networks," in the 4th IEEE Workshop on Mobile Computing Systemsand Applications (WMCSA), 2002.

[9] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, \A secure routing protocol for ad hoc networks," in the 10th IEEE International Conference on Network Protocols (ICNP), November 2002

[10] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, \Secure routing and intrusion detection in ad hoc networks," in 3rd International Conference on Pervasive Computing and Communications, March 2005.

[11] F. Kargl, A. Geis, S. Schlott, and M. Weber, \Secure dynamic source routing," in the 38th Annual Hawaii International Conference on System Sciences, 2005. HICSS'05,January 2005.11

[12] P. Prasithsangaree and P. Krishnamurthy, On a framework for energy-efficient security protocols in wireless networks," in Computer Communications, ser. 17, vol. 27,November 2004, pp. 1716-1729.

[13] R. Vedhavarshini , T. Anand Efficient Data Packet Transmission in MANET Using Enhanced Hybrid Cryptographic Technique(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3309 - 3311

[14] Surya.S.Raju Manjunath.S.S An Efficient Prelude to Measure Packet Loss and Delay Estimate with Elevated Security FeatureInternational Journal of Computer Applications (0975 – 8887)Volume 26– No.3, July 2011.