Indian Journal of Science and Technology, Vol 9(40), DOI: 10.17485/ijst/2016/v9i40/78596, October 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

An Effective (FD-E-TOHIP) Fault Detection Enabled E-TOHIP for Mobile Ad-Hoc Networks

N. Sabiyath Fatima* and V. Muthupriya

Department of CSE, B.S Abdur Rahman University, Vandalur, Chennai - 600048, Tamil Nadu, India;
sabiyathfathima@bsauniv.ac.in, muthupriya@bsauniv.ac.in

Abstract

Objectives: Security is a challenging issue in mobile ad-hoc networks (MANET). The main objective is to implement FD-E-TOHIP Fault Detection Mechanism (FDM) on Enhanced Topology-Hiding Multipath Routing Protocol (E-TOHIP) in mobile ad-hoc networks (MANETs). **Methods/Statistical Analysis:** E-TOHIP do not permit packets to hold routing information. Once a route is recognized, E-TOHIP will publicize a set having the nodes that have been positioned on routes, which prevents a node from being located on another route. It also establishes multiple node-disjoint routes and excludes unreliable routes before transmitting packets. **Findings:** With the help of FDM faults in the network can be easily identified. Message loss due to node permanent fault and message loss due to data transmission are the types of faults that occur here. If the node is considered to be a everlasting fault, then the messages at the node location will get lost and it won't work until a re-establishment is done. The message loss during data transmission occurs due to three kinds of faults namely message redirection, topology change and buffer overflow. **Applications/Improvements:** Along with FDM, various attack implementation is also done in order to test the efficiency of E-TOHIP protocol.

Keywords: E-TOHIP, Fault Detection Mechanism, MANET

1. Introduction

The existing multipath routing protocols in mobile ad-hoc networks ignore the topology-disclosure problem. To overcome the problem of topology disclosure, a new Enhanced Topology Hiding Multipath Routing Protocol (E-TOHIP) is proposed. E-TOHIP do not tolerate packets to bear routing information while sending data. Hence the malevolent nodes cannot infer network topology and initiate various attacks based on that. This protocol also establishes multiple node-disjoint routes during route discovery endeavor and excludes untrustworthy routes before transmitting packets. Similarly E-TOHIP does not hold link connectivity information while sending packets from source to destination. Thus no node can assume network topology by capturing packets and the network topology is concealed.

The Security threat analysis[1] has been done considering parameters like routing information, sniffing, encryption redundancy, etc. The Simulation results focused on the normalization of the data set to obtain maximum and minimum values for classification of the network. The factors involved for classification include delay and bandwidth utilization. The main objective is to propose a new Enhanced Topology-hiding Multipath Routing Protocol (E-TOHIP)[2] for mobile ad-hoc networks (MANETs). E-TOHIP do not permit packet headers to bear routing information, so the malevolent nodes cannot infer the network topology and start various kinds of attacks. Once a route is established, E-TOHIP will demonstrate a set of nodes that has been positioned on routes. This prevents the particular set of nodes from being placed on another route. The network is simulated using NS-2 simulator to evaluate the performance of E-TOHIP and also to compare it with Secure Routing Protocol (SRP).

A new Topology-Hiding multipath Protocol (TOHIP)[3] is proposed to mitigate the problem of topology exposure. TOHIP do not permit the packets to hold routing information while transmitting the packets. The main disadvantage is TOHIP has high routing overhead

*Author for correspondence

because every time while transmitting the packets new and different routes is found between the source and destination node.

Fault propagation model (FPM)[4] is based on random walk model to depict the association performance of the nodes in MANET. In this model, the authority of the average transmission range, the node's number and the size of the simulation areas on MANET's connectivity is considered. The main advantage of using this model can definitely illustrate the overcrowding state of the whole network, and the liability data could be straightforwardly composed from the FPM. A fault tolerant bio-inspired topological control mechanism (TCM-Y)[5] is designed for the evolutionary decision making process of autonomous mobile nodes that adaptively adjust their spatial configuration in MANETs.

A Behavioral approach[6] for detection of malicious attack in MANET uses machine learning to categorize nodes as malicious. A well-organized approach for the discovery of node misconduct[7] in MANET is based on link misconduct and the major benefit of this approach is based on the practice of two techniques. These techniques will be used in parallel in such a way that the results produced by one of them are further processed by the other to lastly create the list of mischievous nodes. Risk-aware mitigation technique[8] for routing attacks in MANET has received a considerable attention because it has caused the most devastating damage to MANET. Here a risk-aware mitigation technique is proposed to systematically cope with the identified routing attacks. This risk-aware approach is based on an extended Dempster-Shafer (DS) mathematical theory of evidence. The problem of packet dropping attack or black hole attack is addressed and three defense line schemes to mitigate packet dropping attack[9] is proposed. The first defense line scheme is mainly used for prevention purpose. It aims to forbid the malicious nodes from participating in packet forwarding function.

A novel fault detection mechanism named REW (Reverse-inhibition Early Warning)[10] is proposed, which can send warning message before the buffer data are consumed away to avoid the termination of service. It can reduce the number of repetitive and wrong warning through reverse-inhibition strategy at the same time which is a main advantage here. A policy-based malevolent peer discovery method[11] is planned and developed, in which framework information, such as announcement channel rank, buffer status, and transmission power level, is collected and then used to determine whether the misconduct is likely a consequence of malevolent action or not.

A novel route discovery algorithm[12] called endair A addresses the hidden channel attack problem and the main objective of this algorithm is to find a route that is a suitable communication channel. The route discovery process here can be either proactive or reactive. While transmitting the packets the adversary does not have full control of message delivery schedule instead the adversary may prompt honest parties to initiate new route discoveries which is a major drawback .An omission fault model[13] evaluates the significant number of broadcasting protocols in MANET under a realistic scenario of momentary failures and topology changes. Here in this model faulty node will fail to send messages with large payloads, such as broadcast messages, but will still be able to exchange neighborhood and control messages. The main disadvantage is the exact number of nodes that fail on any given run depends on the percentage of failed nodes.

A path survival algorithm[14] addresses the difficulty of protected and fault-tolerant communication in the existence of adversaries across a multi-hop wireless network with often varying topology. The main advantage of SMT and SSP is it robustly detects transmission failures and continuously configures their operation to avoid and tolerate data losses, and ensures the availability of communication. SSP provides feedback across a single route and switches to a new route only after the current one is deemed failed..SSP transmits data across a single route, and does not perform data transmission which is a disadvantage. An authenticated routing in ad hoc networks (ARAN)[15] mitigate the problem of finding paths in very dynamic networks without considering security. The main advantage is ARAN introduces authentication, message integrity, and non-repudiation to routing in an ad hoc environment as a part of a minimal security policy. The major disadvantage is the cost of ARAN is larger, which result in a higher overall routing load, and higher latency in route discovery because of the cryptographic computation.

Collaboration-based content adaptation middleware called ConAMi[16] is distinct that make information fit with the framework of the user and his/her surroundings. It also projected fault finding and recovery method to improve middleware ConAMi. However, in a active pervasive computing surroundings, the amalgamated service can be unsuccessful very effortlessly due to the mobility of services' owners which is main disadvantage. To ensure

highly reliable service composition, the middleware ConAMi considers the TTL of a service during services assortment which is a major advantage.

A routing framework[17] is proposed for providing robustness to node failures in mobile ad hoc networks. The major disadvantage is when distances between sources and destinations increase, bottlenecks inevitably occur and thus, the possibility of finding multiple paths is considerably reduced. The major advantage is relationship between the number of node-disjoint paths can be found between a source and a destination and also the density of nodes in the network. The stable node-disjoint multipath routing (NDMR) protocol[18] is proposed to decrease the overhead in mobile ad hoc networks. The main goal of NDMR is to build multiple node disjoint paths with a low routing overhead during a route discovery.

2. Materials and Methods

In the proposed system, in order to identify the faults that occur in the network Fault Propagation Model (FPM) of mobile ad hoc network (MANET) is implemented based on random walk model. Based on this model, the authority of the standard broadcast range, the node's number and the size of the simulation areas on MANET's connectivity is considered. Message loss due to node permanent fault and message loss due to message sending are the faults that occur here. If the node is enduringly liability, the messages in the node will get lost and it can't work until a re-establishment is done. The message loss during message sending consist of three kinds of faults namely message redirection, topology change and buffer overflow. Also along with FPM various attack implementations is also done in order to test the efficiency of E-TOHIP protocol. The advantages are Fault data could be directly collected and also resist against attacks.

2.1 Architecture Diagram

The different phases and process of FD-E-TOHIP is depicted in the Figure 1. In FD-E-TOHIP the route discovery process is initiated by the source node by sending the route request packets to its neighbors. upon receiving a route request message, every intermediate node creates a reverse route, and rebroadcasts the message if it has never received this message before.

Similarly route reply message (RREP) is transmitted from the destination node to the source node via

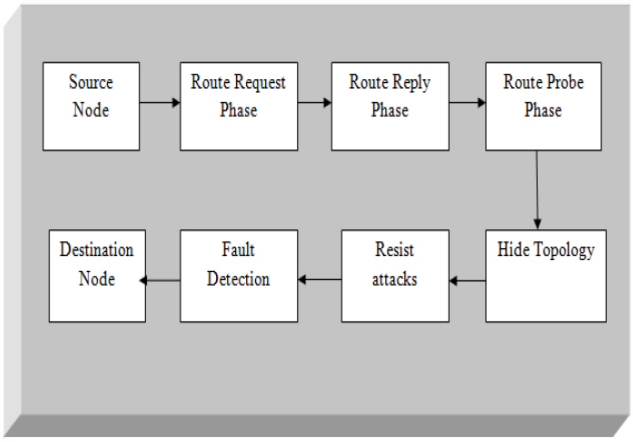

Figure 1. Architecture Diagram.

broadcasting. Upon receiving such a message, an intermediate node selects the neighbor adjoining to the source node as the preceding hop on the route. It then advertise this assortment to all its additional neighbors, to make sure no node is chosen on many routes. It is only in this phase where the topological information is hidden by creating many node-disjoint routes. Finally the source node sends a route probe message through every discovered route to the target node in order to sense and eliminate the untrustworthy routes earlier than transmitting the packets. The above said process is done iteratively in order to hide the topological information from the unauthorized users. Only after performing the above operations the packets is transmitted from the basis node to the end node. While transmitting the packets E-TOHIP resist against a variety of attacks.

At the end fault detection mechanism is implemented in order to find various kinds of faults that occur in the network. With the help of fault detection mechanism, fault propagation model (FPM) is being implemented in order to find message loss due to node failure and the message loss caused while transmitting the message. Fault Detection Mechanism with Enhanced Topology hiding multipath routing protocol (FD-E-TOHIP) consist of two phases.

Implementation of Replay attack-An attacker can carry out a replay attack by recording old valid control messages and re-sending them, to make other nodes bring up to date their routing tables with stale routes. This attack is winning even if control messages tolerate a digest or a digital signature that does not comprise a timestamp.

Implementation of fault detection mechanism-With the help of fault detection mechanism, Fault Propagation

Model (FPM) is being implemented in order to find message loss due to the node failure and the message loss caused while transmitting the message.

2.1.1 Fault Detection Enabled Enhanced Topology Hiding Multipath Routing Algorithm (FD-E-TOHIP)

The main objective of the E-TOHIP algorithm is to hide the topological information and the corresponding link information in order to defend against various kinds of attacks[4].

2.1.2 Implementation of Replay Attack

Upon the ETOHIP protocol replay attack is implemented. Since ETOHIP can hide network topology, malicious nodes cannot launch attacks from central positions of the network. Thus, the potential damages incurred by malicious nodes are greatly reduced or even eliminated. A replay attacker performs this attack by interception and retransmission of the valid signed messages. The validation of signed messages is verified by a timestamp discrepancy fixed by sender and receiver nodes. To avoid such situation E-TOHIP verifies the time stamp of the communication duration between sender and receiver nodes.

In the Figure 2 initially the source node S sends the route request packet to the destination node D for particular path traversal. This route request packet will be sent continuously until the packets reach the particular destination node D. Once it reaches the destination node D a corresponding route reply packet is sent to the source node S. While sending the route reply packet the attacking node H sends it as if it is the destination node. The source node S discards the packet coming through the path D→I→H→c→S because the attacking node H doesn't have the particular field format.

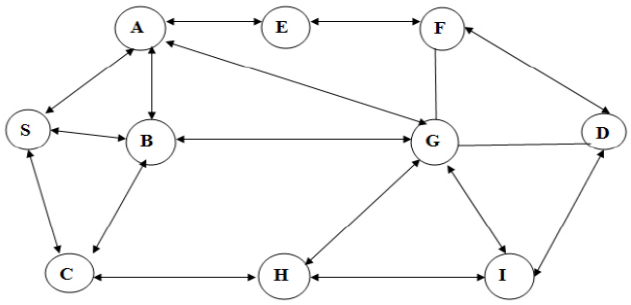

Figure 2. Reply Attack Process.

Every packet that is sent from source to destination has a particular field format and along with it the time-stamp will be attached. In general the attacking node H doesn't have the default packet format and also don't have the correct timestamp value. So due to this the source node S discards the packet.

Pseudo code for Replay attack is as follows,

```
If (string compare ( argv[1], "reply") == 0) then
    Assign reply →index
return packet
end if
void TOHIP::receive node (Packet p, Handler)
        if (ch->ptype() == PT_TOHIP) then
                Assign default packet format ih->ttl = 1
                recvTOHIP(p)
                return
end if
        / Check if a packet is originating../
if((default ih->source addr() == index) &&(ch->num_
forwards() == 0)) then
        / Add the IP Header/
ch->size() + → IP_HDR_LEN
if ( (u_int32_t)ih->daddr() != IP_BROADCAST) then
assignih->ttl_ = NETWORK_DIAMETER
        else if (reply == index) then
                drop (p, DROP_RTR_ROUTE_LOOP)
                return
end if
end if
```

In the above mentioned pseudo code initially the destination node D checks the incoming packet has correct packet format or not. If it has a correct packet format then it creates route to the source indicating that it is the corresponding destination node. If the arriving packet doesn't have the default packet format then destination node doesn't create the routes.

After creating the routes, the packets are sent from the destination node to the source node. In the mean time an intermediate node acts as a attacking node and sends fault information saying that it is the intended destination node. Source S discards the packet that is arriving through the intermediate attacking node. The source node S identifies the attacking node by checking the packet format. Also every node checks for the default packet format. Here the intermediate attacking node doesn't have the default packet format instead it has a different one. So due to this the source node S stops accepting the packets coming

from that route and takes a different route for sending the packets. Thus, E-TOHIP is said to be an highly efficient protocol because it can resist against this attack.

2.1.3 Implementation of Fault Detection Mechanism (FD-E-TOHIP)

A Fault Propagation Model (FPM) is designed and developed based on random walk model. With the help of Fault Detection Mechanism (FDM) the failures that occur in the network and the node movement behavior can be easily identified. Every node has a wireless exposure area, only within which the other nodes be capable of receiving the message from inside. According to the elementary principle, the region that a wireless node be able to launch message is a spherical. There is no permanent midpoint in MANET, and every node can move about freely.

As a consequence, the network topology may perhaps transform rapidly and it is volatile over time. Two types of fault occurs, one is the message loss due to node permanent fault and message loss at the time of sending message. If the node is hypothetical to be a enduring fault, the messages in the node will be misplaced and it will not work until a re-establishment is taken. In the second technique message loss occurs during data transmission due to message redirection, topology change and buffer Overflow. Due to the random walk association of the nodes in the cell space, the physical topology changes each and every time period.

Fault Detection Mechanism is implemented on E-TOHIP protocol (FD- E-TOHIP). Once the protocol gets executed, FDM easily finds fault in the network. Generally in MANET, when the attacker gains control over network, the attacker tries to capture the packet that is being sent from source to destination. FDM can easily differentiate whether a node is a malicious node or not. This can be easily determined once a route is established between the source and destination.

When a packet is sent between the established routes the faulty nodes can be identified. Each packet that is being sent from source to destination has a particular default packet format. When this default packet format varies the faulty nodes can be identified with it and link with that node will be broken. This is because the attacking node has different packet format. Again a new route is established by beginning a new route discovery process. With the help of FDM, this fault can be easily identified and implementing FDM on E-TOHIP increases the efficiency of node.

Pseudo code for FD-E-TOHIP

```
Void TOHIP::handle_link_failure(nsaddr_t id)
For (rt = rtable.head(); rt; rt = rtn) then // for each rt entry
TOHIP_Path path
        Assign rtn = rt->rt_link.le_next
if((rt->rt_flags == RTF_UP) && (path=rt->path_lookup(id)) ) then
checkif assert ((rt->rt_seqno%2) == 0) then
rt->path_delete(id)
        if(rt->path_empty()) then
         Assign rt->rt_seqno++
         Assign rt->rt_seqno = max(rt->rt_seqno, rt->rt_highest_seqno_heard)
// CHANGE
if (rt->rt_error) then
        Assign re->unreachable_dst[re->DestCount] = rt->rt_dst
        Assign re->unreachable_dst_seqno [re->DestCount] = rt->rt_seqno
re->DestCount += 1
rt->rt_error = false
end if
rt_down(rt)
end if
end if
end if
```

In the above mentioned pseudo code link failure in the network can be easily identified. Initially routing table's entry is checked for the routes that are established. When an attack takes place in the network while sending a packet from source to destination, link from the corresponding attacking node will be discarded and a alternate new route will be established by initiating new route discovery process. Once the link is cut from the attacking node with the help of FDM a alert is generated that a link failure has occurred. Then the packets are sent to the source through newly established routes. E-TOHIP proves to be a highly secure and resistant protocol because when a attack takes place in a network,, it gives an alert to the network that a fault had occurred and entirely takes a different route for transmitting the packets by initiating a new route discovery process. The efficiency of E-TOHIP protocol is further tested by taking into account the performance metrics like Packet Delivery ratio (PDR), End to End delay (E2E).

4. Results and Discussions

The analysis and implementation of fault detection enabled Enhanced Topology hiding multipath routing protocol (FD-E-TOHIP) is carried out using network simulator NS2.In this simulation, the experimental model is built on 100 nodes and the mobile nodes pursue the random way point mobility model. The channel capability is 2 Mb/s and the highest communication range is 250 m.

The performance comparison is done between FD-E-TOHIP in adversarial and non-adversarial scenarios in order to test the efficiency between them. This performance comparison is done by taking into account the performance metrics like packet delivery ratio (PDR), routing overhead (ROH), end to end delay (E2E). While making comparison FD-E-TOHIP is proven to be highly secure in both the scenarios. The parameters like end to end delay, packet Delivery Ratio, etc can be plotted using trace graph.

These metrics are calculated by taking into account the number of sending packets, number of receiving packets at destination and considerably the number of routing packets which is generated in the trace file. The PDR ratio is high because FD-E-TOHIP securely sends the packets even in attacking scenarios by establishing the node-disjoint routes. This is done by establishing three routes for every packet transformation. The first route is used for sending the route request packets. Second route is used for sending the route reply packets and finally the third route is used for sending the actual data packets. The end to end delay of FD-E-TOHIP also initially increases and then it decreases. This is because of finding new routes for each packet transmission. But once the route is found the packets are immediately transferred between the source node and the destination node in a secure way.

The simulation analysis of FD- E-TOHIP protocol is obtained by considering the performance metrics like Packet delivery ratio and End to End delay.

Packet Delivery Ratio (PDR) is the total amount of packets acknowledged by the recipient and quantity of data packet sent by starting place. The formula to calculate the packet delivery ratio is,

$$PDR = \frac{\sum \text{Data packet acknowledged by the target recipient} * 100}{\sum \text{Data packet sent by the starting place}}$$

While making comparison FD-E-TOHIP considerably has almost similar packet delivery ratio in both the scenarios. The comparison is done by taking speed in x-axis and packets in y-axis. Then by taking into account the number of sending packets, receiving packets and routing packets the graph is plotted and is referred in figure 3. The PDR comparison between FD-E-TOHIP in adversarial and non- adversarial scenarios which is shown in the graph is similar in both the cases.

The main reason for PDR to be similar in both the cases is implementation of fault detection mechanism in E-TOHIP. Also E-TOHIP securely send the packets by establishing the node-disjoint routes. This is done by establishing three routes for every packet transmission. The first route is used for sending RREQ packets. Second route is used for sending the RREP packets and finally the third route is used for sending the actual data packets. With the help of Fault Detection Mechanism (FDM) faults in the network can be easily identified. FDM is also considered as one of the factor for the packet delivery ratio to be high. Thus while considering packet delivery ratio E-TOHIP is considered to be highly efficient in both the adversarial and non-adversarial scenarios.

End to End delay (E2E) is defined as the average time taken by a data packet to arrive at the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Here only the data packets that are successfully delivered to destinations are taken into account. The formula to calculate end to end delay is defined as follows,

$$E2E = \frac{\sum \text{End to End delay for each data packet}}{\sum \text{Data packet received by the destination}}$$

While comparing FD-E-TOHIP is said to have higher end to end delay in attacking scenario because when an attack takes place, the attacking node tries to send the packet to destination continuously which is referred in figure 4. These simulations result is plotted in x graph by taking speed in x-axis and the packets in y-axis.

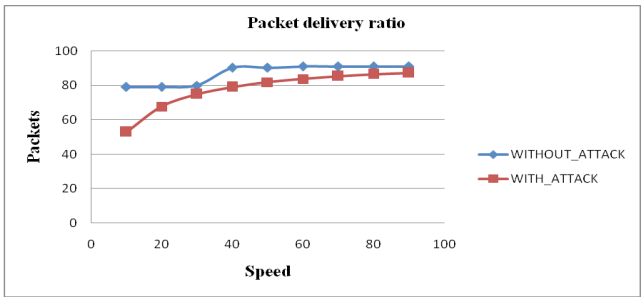

Figure 3. PDR comparison of E-TOHIP in adbversial and non--adversial scenarios.

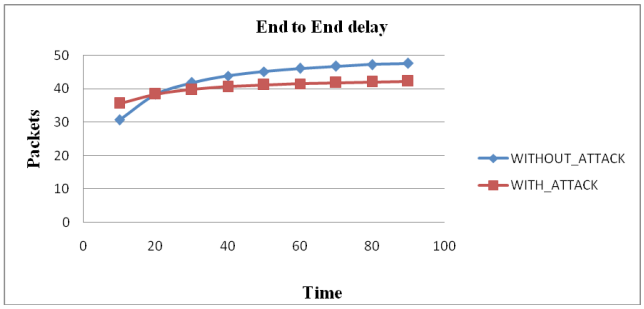

Figure 4. E2E comparison of E-tohip in adversial and non-adversial scenarios.

Thus packet delivery ratio (PDR) and end to end delay (E2E) metrics comparison of E-TOHIP is made in both adversarial and non-adversarial scenarios. And finally when analyzing, FD-E-TOHIP is proven to be highly secure in both the attacking and non-attacking scenarios.

5. Conclusion

In order to agreement with the topology-disclosure difficulty, a new Enhanced Topology-Hiding multipath routing Protocol (E-TOHIP) is designed and developed which does not contain association information in route messages at the time of transmission of the packets. In the E-TOHIP protocol, fault detection mechanism is implemented with which faults in the network can be straightforwardly recognized and vigilant is generated. Along with it, evaluation of FD-E-TOHIP is done in both adversarial and non-adversarial scenarios. Thus, by capturing route messages, no node can deduce network topology and the network topology information is hidden. Simulation results and analysis shows that E-TOHIP is proven to be highly secure and efficient routing protocol.

FD-E-TOHIP can be extended further by implementing various kinds of attacks like Sybil attack, modification attack along with fault detection mechanism with which the efficiency of the FD-E-TOHIP protocol can be further improved.

6. Acknowledgement

We owe a debt of gratitude to the management and the Department of computer science and engineering of B.S. Abdur Rahman University for their support to complete this work.

7. References

1. Vijay I, Rath AK, Puthal B. Exploration of security threat analysis in wireless mobile Ad Hoc Networks. Indian Journal of Science and Technology. 2016; 9(35):1–11.
2. Neeraja E, Sabiyath Fatima N. Security Enhancement in MANET Using A New Enhanced Topology Hiding Multipath Routing Protocol (E-TOHIP). International Journal of Applied Engineering Research. 2005; 10(20). ISSN 0973-4562.
3. Zhang Y, Yani T. TOHIP:A topology-hiding multipath routing protocol in mobile ad hoc networks. IEEE Ad Hoc Networks. 2014; 21:109–22.
4. Hong S, Yang H. Fault Propagation Model in Mobile Ad Hoc Network Based on Random Walk Model. IEEE Cyber Technology in Automation. 2014; 22(2):376–85.
5. Gundry S, Zou J. Fault Tolerant bio-inspired Topology control mechanism for autonomous mobile node distribution in manets. IEEE Trans Mobile Computing. 2013; 10(9):1345–58.
6. Patel M, Sharma S. Detection of Malicious Attack in MANET A Behavioral Approach. IEEE, Computer Science Engineering. 2012; 183–210.
7. Samreen S, Narasimha G. An Efficient Approach for the Detection of Node Misbehaviour in a MANET based on Link Misbehavior. IEEE Computer Networks. 2012; 9(16).
8. Zhao ZM, Hu HX. Risk-aware mitigation for MANET routing attacks. IEEE Trans Depend Sec Comput. 2012; 9(2):250–60.
9. Djahel S, Nait-Abdesselam F. Mitigating packet dropping problem in mobile ad hoc networks: proposals and challenges. IEEE Commun Surv. 2011; 13(4):658–72.
10. Cui J, Wu L. A Novel Fault Detection Mechanism of Topology aware ALM. IEEE Computational Intelligence and Industrial Applications. 2009; 98(76):135–40.
11. Li W, Joshi A. Policy-based Malicious Peer Detection in Ad Hoc Networks. IEEE Computer Science and Engg. 2009; 87(62):456–60.
12. Burmester M, Medeiros B. On the security of route discovery in MANETs. IEEE Trans Mob Comput. 2009; 8(9):1180–8.
13. Oliveira T, Greve F. The Node Reliability Approach to Broadcasting in Manets: Raising Reliability With Low End-to-End Delay. IEEE Ad hoc networks. 2007; 1(3):89–102.
14. Papadimitratos P, Haas ZJ. Secure data communication in mobile ad hoc networks. IEEE Journal on Selected Areas in Communications. 2006; 24(2):343–56.
15. Sanzgiri K, Dahill B. Authenticated routing for ad-hoc networks. IEEE Journal on Select Areas communication. 2005; 23(3):598–610.

16. Fawaz Y, Bognanni C. Fault Tolerant Content Adaptation for a Dynamic Pervasive Computing Environment. IEEE Computer Networks. 2005; 12(9):120–7.
17. Ye Z, Krishnamurthy SV. A routing framework for providing robustness to node failures in mobile ad hoc networks. IEEE Ad Hoc Netw. 2004; 2(1):87–107.
18. Li X, Cuthbert L. Stable node-disjoint multipath routing with low overhead in mobile ad hoc networks. IEEE Annual International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunications Systems (MASCOT). 2004; 184–91.