Packet Forwarding Misbehaviour Isolation using Fuzzy Trust-based Secure Routing in MANET

Jenish R.Gandhi
Department of Computer Engineering / IT
SVM Institute of Technology
Bharuch 392-001, Gujarat, India

Rutvij H. Jhaveri
Department of Computer Engineering / IT
SVM Institute of Technology
Bharuch 392-001, Gujarat, India

ABSTRACT

MANETs are much more susceptible to various attacks because of openness in network topology and being away of a centralized administration in management. As an outcome of that, more malicious nodes are often comes in and goes out without being detected from the network topology. Hence, MANET needs very specialized security methods to isolate the false entrance. As well as there is no single solution that fitting in different types of the network where the nodes can be behave like any apparatuses. The networks works well if the nodes are trusty and act rightly cooperatively. In order to improve the security of the network, this paper gets started the new interesting approach to evaluate the trustworthiness of the nodes. Fuzzy Trust-based Secured Routing (FTSR) approach provides a flexible and feasible approach to choose trusted route to meet the requirement of the security of the data transmission. In this, fuzzy logic rule prediction mechanism is adopted to notice the future behavior of node by updating the node's trust. We have also analyzed the performance metrics such as packet delivery ratio, end-to-end delay and average throughput which can also increased accordingly through newest approach.

Keywords

Trust, MANET, Security, AODV, Fuzzy Logic, FTSR

1. INTRODUCTION

A self-configuring and self-organizing network architecture in which different mobile devices are connected by wireless link is called MANET [1]. MANET is a less-infrastructure [2] in which mobile nodes are moving arbitrary without any managerial dependent. As an outcome, topology may change frequently at unpredictable times. Mobile devices in ad-hoc network are connected via wireless links. Therefore, quantifying a trust value is major issue because ad-hoc networks depend on cooperative and trust nature of nodes. Due to the energetic nature of the nodes, the degree of trust additionally changes.

On another side, Security [3] is additionally main concern to function the network congruously where message can altered through the third party. In other words, we can verbally express that the security issue have been met by achieving the availability of the network services, confidentiality and integrity of the data. MANETs suffers from several security attacks due to have several feature such as dynamic topology, lack of central coordinator, cooperative algorithms. Wireless links are much more susceptible to sundry attacks which makes easier for attacker to go inside and come outside without being detected. Hence, we can verbalize that security of MANETs is cry of the day. In order to provide secure and reliable communication and transmission, the researcher has to get clearly the variants of threat and there affect on MANETs. Moreover, MANETs are open for different threat because communication is based on different nodes which have a mutual trust in one another.

In a packet dropping attack, the malicious nodes always reply positively to route request whether it may not have valid route toward the destination. Because of this, all traffic within the neighborhood of malicious nodes is diverted towards malicious nodes which drop the entire packet passing from resulting in denial of services.

For prosperous communication or transmission, it is compulsory to observe the node's behavior whether node will take part or not. For this, paper establishes incipient approach FTSR which utilizes a fuzzy logic rules. Fuzzy logic is a computational paradigm that builds a set-of user-defined human language rules which are converted into mathematically equivalents to handle the quandary of imprecise and incomplete data. In other words, Fuzzy logic deals with approximate reasoning rather than fixed and exact reasoning. The fuzzy logic may have truth value which has a range in between 0 and 1. The benefit of this system is flexibility and simpleness.

The newest approach avoids the inclusion of misbehaving node during route establishments by using the trust metrics. The FTSR categorized the misbehaving nodes and trustworthy nodes according to fuzzy levels such as very trustworthy, trustworthy, untrustworthy, and Very untrustworthy which is represented by the trust values. After getting the nodes trustworthiness, FTSR utilizes the fuzzy inference rules based on fuzzy levels for secure routing.

The rest of the paper is organized as: chapter 2 provides the illustration of previous related works. The newly method of proposed scheme is mentioned in chapter 3. The simulation parameters that is suited for newly approach to get the best result is described in chapter 4 and chapter 5. At last, the paper concluded the results.

2. RELATED WORK

We have survey many research paper [4] on the basis of trust management and fuzzy logic. Some of important paper is define as below:

Srinivas Sethi et al. [5] proposed FTAR that utilized ACO (Ant-Colony Optimization). The food-searching algorithm of real ant-agent is called ACO. FTAR is using two parameters such as Time-ratio and Dropped packet to categorized the healthy and malicious nodes. Fuzzification utilized the time-ratio which is ratio between the route-reply time and time-to-live. It withal access dropped packet parameter utilized to measure the number of packet dropped at node. FTAR utilizes the ACO by using two types of control packet: BANT and FANT.

N.Marchang et al. [6] Light-weight means estimating the trust that one node has for another. In this, every node maintains the trust value for its neighbor node. The trust value can be habituated to quantify the trust of neighbor node. For this each neighbor node contains the three data structures: ToForward, Forwarded, Source list.

Hui Xia et al. [7] TSR is the on-demand trust-based unicast routing protocol which is flexible to find the optimal route for secure routing. TSR that contains four major blocks: Route discovery, Trust computation, Trust application and Route maintenance. Trust computation contains two processes: Computation of node's historical trust and node's current trust. In node's current trust, the trust value of node current position is computed by fuzzy logic rules prediction method. Trust application contains three processes: Route discovery, Route update and Route handoff process. The secure routing path is chosen based on minimum trust value of the route.

Radha Krishna Bar et al. [8] the computation of trust value is depending upon two properties such as packet forwarding ability and weight factor. The weight factor measures through the number of RREQ received and through the number of RREP sent. After calculation, this trust value is inserted into the routing table and route discovery is done based on this trust values rather than the traditional shortest path. During the route establishment less trusted node can be avoided in AODV routing protocol.

Suparna Biswas et al. [9] Trust evaluation of every node is defined by three parameters: Rank, Remaining battery power, and Stability factor. Rank measures the reliability of the node. Rank of node drops to 0 defined the node is untrusted or malicious node. Remaining battery power of node is considered at a certain time, Stability factor includes two parameters: (i) Pause time (Tpause) and (ii) Velocity for node is defined by Vmax.

Hui Xia et al. [10] proposed FAPtrust define the multiple trust decision factor based on fuzzy theory. AHP theory based on entropy weight factor used to calculate the multiple decision factors and utilize the fuzzy logic prediction rules for compute the node's trust value. In this, author establishes two types of trust, namely, direct and indirect trust. The new approach establishes the trust relationship based on entropy weight method and fuzzy logic rules prediction mechanism. Fuzzy logic theory is suitable for define the uncertainty and imprecision of the network. In node's current trust, the trust value of current position of node is computed by the fuzzy logic rules prediction method.

3. PROPOSED SYSTEM

In this section we introduced the improvement of the selection of most secure and reliable route by establishing the trust management [4] between the nodes. As well as, we also define the fuzzy logic rule prediction method to detect the secure route by isolating the evil nodes.

The steps of most incipient scheme is defines as below.

3.1 Before Packet Transmission Process

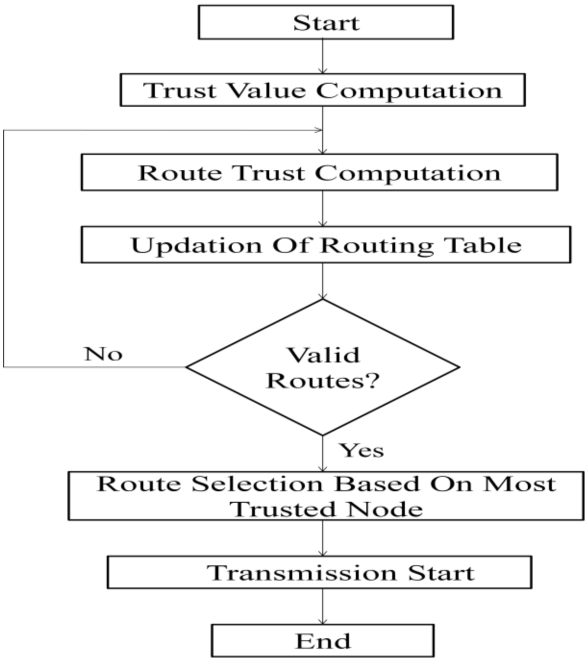


Figure 1: Before Packet Transmission Process

1. In our trust model, each node maintain trust value for its neighbor node.

   Calculate the level of trust value

   $$T_i(j) = \alpha T_{i(self)}(j) + \beta T_{i(neighbor)}(j)$$

   Where, $T_i(j)$ is the trust of node i on neighbor node j.

   $T_{i(self)}(j)$ represent the trust of node i on node j.

   $T_{i(neighbor)}(j)$ represent the trust that neighbor of node i has on node j,

   and, α, β are weighting factor ($\alpha + \beta = 1$ and $\alpha >= 0, \beta <= 1$)

   Let $a_1, a_2, a_{3...} a_n$ be the neighbor of node i such that they are also node of j and n is the number of neighbor node, than trust value can be calculated as,

   $T_{i(neighbour)}(j) = \frac{1}{n} \sum Ta_k(j)$

2. In trust model, routes that are established which are withal associated with the trust value. It designates routes are nothing that the sequence of the nodes.

   Let r is consider as a route and l nodes are represented as a sequence $a_1, a_2, a_3, ..a_l$ than the trust value of routes are represented by the R_r

   $R_{r\,=}\ Ta_1(a_2)\ Ta_2(a_3) \ldots Ta_{l-2}(a_{l-1}) = \prod Ta_{i-2}(a_{i-1})$

3. For a neighbour node, we have establishes a three data structures: ToForward, Forwarded, and Source List.

   ToForward: it is utilized to store the number of packet to be forwarded.

   Forwarded: it is utilized to store the number of packet that are already forwarded.

   Source List: it is utilized to define the progenitor of the packet to be forwarded.

Each above data structures is divided into N slots or windows. Each window or slot the positive integer value called a number of packets. The maximum number of packets that each window can store have a fixed size number, M. M and N are define as a configurable parameters. The windows or slots are defined in circular fashion. We have additionally defined the CurrentWindow for two data structure which is utilized to point the current window or slot in both data structure. Initially, The CurrentWindow can set any number between 0 to N-1.

Surmise those promiscuous nodes are take place into the communication. If we consider node i as a promiscuous node in the communication, it watched for two kinds of action of node j. Firstly, node i watches for the packet that is sent to the node j which is to be forwarded further. And secondly, node i watch for the packet that is forwarded by neighbor of node i to the node j. In this both cases, whenever node i find that node j has received the packets which is to be forwarded further than ToForward count of node j is incremented by one. In another case, whenever node finds that node j has forwarded that packet which is received than Forwarded count is incremented by one. If both count is exceeded the limit M than incipient window will be initialized.

3.2 During Packet Transmission Process

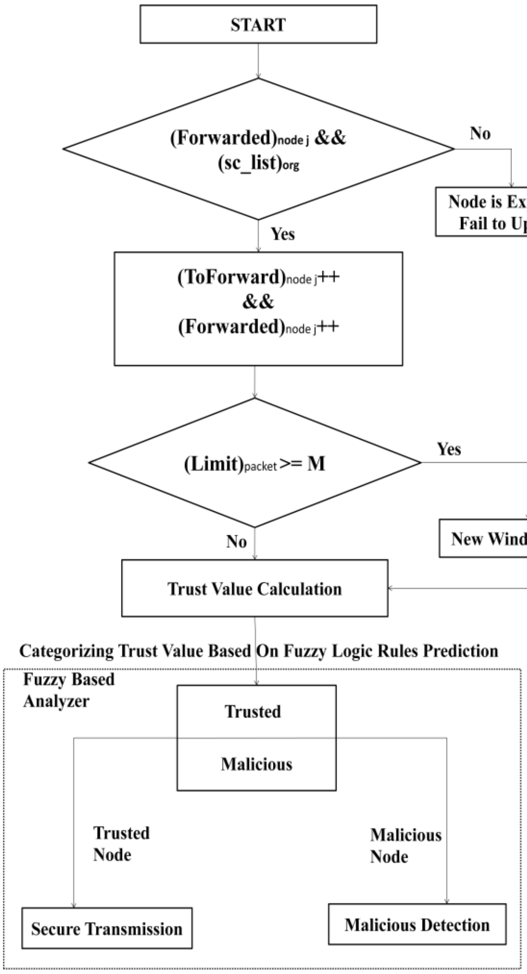


Figure 2: During Packet Transmission Process

Thus, above explicated overall process occur during the packet transmission which is expounded in algorithm as below:
Promiscuous node maintains the Source List (sc_list) and observes the source of the packet.

```
If [(Forwarded) node j and (sc_list contains progenitor node)]
        (Forwarded) node j++;
        (ToForward) node j++;

        If [((Forwarded) node j>=M or (ToForward) node j>=M]
                (CurrentWindow + 1) mod N = 0;
        Else
        Trust Value Calculation:
      $T_{i(self)}(j)=\sum_{k=0}^{N-1} Forwarded(k) \,/\, \sum_{k=0}^{N-1} ToForward(k)$

Else
```

Promiscuous node fail to update Forwarded and ToForward count of node j or progenitor node is not in sc_list

3.3 Current Behavior Observation Using Fuzzy Logic Rules Prediction Method

Fuzzy logic provides ability to handle uncertainty and imprecision effectively. Fuzzy logic based algorithm for trust has been devised and it is applied to the calculated trust value of the nodes. Trust values are computed based on $T_{i\ (self)(j)}$. These values are treated as fuzzy input variables and the Fuzzy logic based algorithm marks the nodes as either trusted or malevolent.

1. Trust value calculation
   $T_{i\ (self)}(j) = \sum_{k=0}^{N-1} Forwarded(k) \,/\, \sum_{k=0}^{N-1} ToForward$

2. Fuzzy Based Analyzer verifies the trust value of the requesting node and performs a look up in the fuzzy table for the fuzzy trust value. Fuzzy Based Analyzer determines the node as TRUSTED or MALICIOUS.

Table I: Fuzzy Discrimination

Fuzzy level	Trust Value	Semantics
1.High	0.8 to 1	Trustworthy
2.Medium	0.6 to 0.8	Trustworthy
3.Low	0.4 to 0.6	Trustworthy
4.Very Low	0 to 0.4	Untrustworthy

3. Fuzzy Inference rules can be applied based on trust-levels to detect untrustworthy node.

   IF Trust value is High THEN node is trustworthy

   IF Trust value is Very Low THEN node is malicious

3.4 Future Behavior Observation Using Fuzzy Logic Rules Prediction Method

When node A sends a request packet to another node B, it’s hard for node A to evaluate whether the node B is willing or not to provide service. For this,

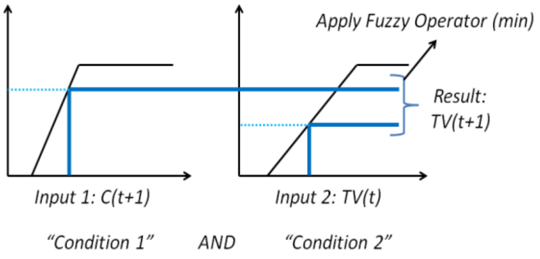
1. Consider TV(t) and C(t+1)

Where, TV(t): Historical trust value at t time interval

C(t+1): Node's capability level at t+1 time interval.

Node's capability level can be achieved through providing the services such as remaining utilization of ratio of battery [11].

2. Apply fuzzy operator



IF Capability level is X AND Trust value is Y THEN TV(t+1) = min(X,Y)

3. Compare trust value TV(t+1) with static threshold value

```
If (TV(t+1) >= TValue)
    Node is Trustworthy
Else
    Node is Malicious
```

Node's trust value will not be updated into the routing table or trusted node will be considered during the transmission process.

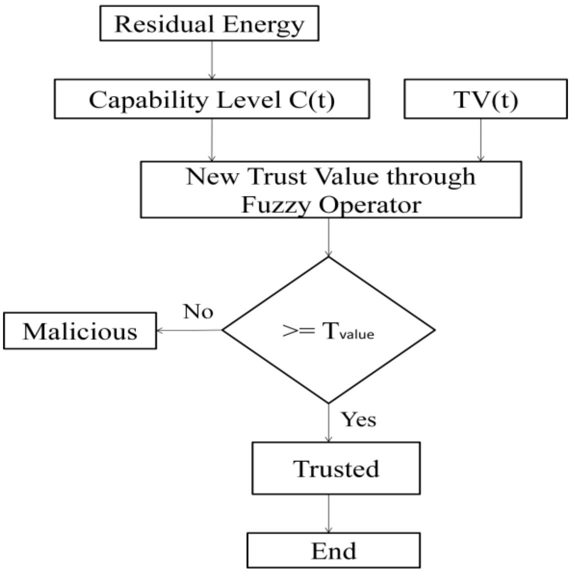


Figure 3: Future Behaviour Observation using Fuzzy Logic Rules Prediction Method

4. SIMULATION PARAMETER

The simulation parameter is explained as below which is used to produce the simulation suite for proposed solution.

Table II: Simulator Parameter

Parameter	Values
Simulator	NS 2.34
Routing Protocol	AODV, FTSR-AODV, Packet Dropper
Scenario Size	800 X 800
Number of Nodes	10, 20, 30, 40, 50
Misbehaving Nodes	3, 6, 9, 12, 15
Simulation Time	600 s
Traffic Type	Constant Bit Rate (CBR) / UDP
Packet Size	1000 bytes
Packet Rate	4 packets/sec
Number of connections	6
Pause Time	10 sec
Maximum Speed	20 m/sec

To overcome of problem of this paper, NS 2.34 simulator was used with 800 X 800 scenarios size. The routing protocol is used in the network for secure routing is called AODV. The packet size is taken 1000 bytes.

We have analyzed the performance parameter such as packet delivery ratio, end to end delay, average throughput, normalized routing overhead and average energy consumption to evaluate the performance of the routing protocol. Also we analyzed the result with packet dropping attack. The attacker model is define as below which forward the 70% packets and drop the 30% packets with destination sequence number. Remember our approach able to detect packet dropping attack.

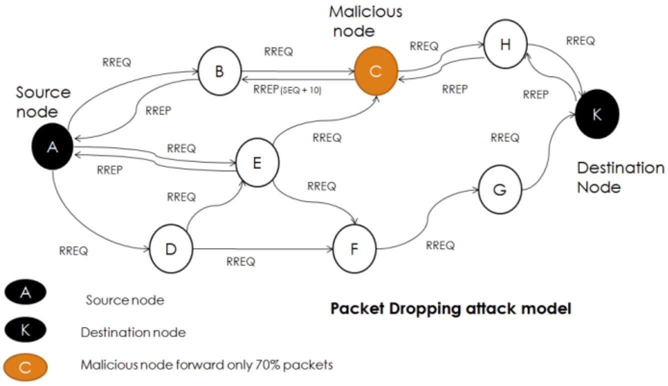


Figure 4: Attacker Model (Packet Dropping Attack)

5. EXPERIMENTAL RESULTS

5.1 Packet Delivery Ratio:

In this, the PDR of packet dropping attack is decreases with compare to the proposed scheme. To overcome of problem, we have taken 30% of malicious nodes in packet dropping attack to analyze the parameter. The below figure describes the comparison between the proposed scheme and packet dropping attack with respect to PDR.

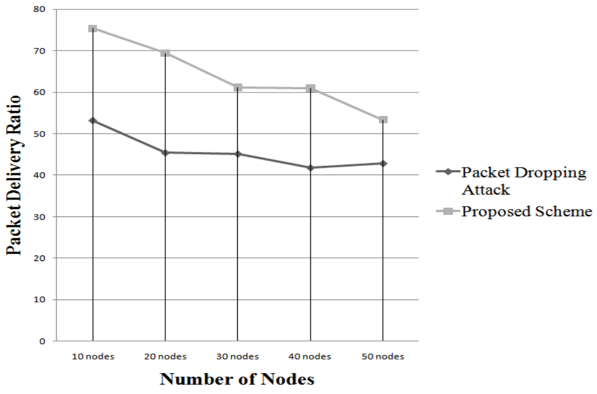


Figure 5: Packet Delivery Ratio (30% Packet Dropper)

5.2 End to End Delay

It measure the average delay time that is taken by data packet between sources to destination. In this, the delay is increased in packet dropping attach with compare to proposed scheme.

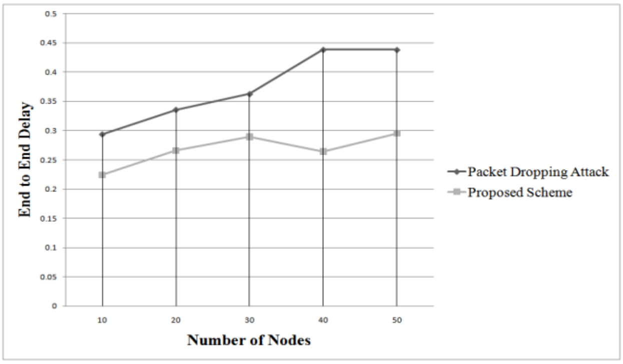


Figure 6: End-to-End Delay (30% Packet Dropper)

5.3 Average Throughput

It measure the average of successful packet transmission from source to destination over a communication channel. In this, the performance of the network is increased in case of proposed scheme.

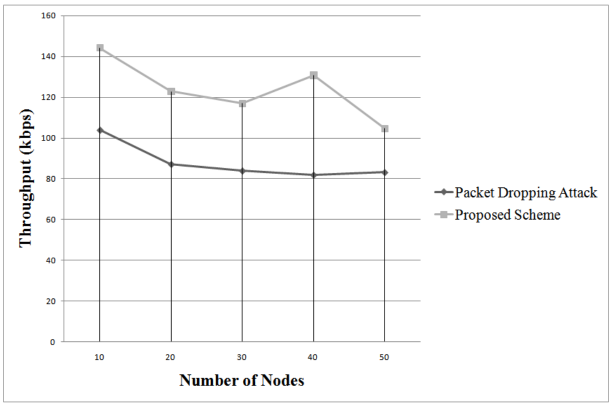


Figure 7: Average Throughput (30% Packet Dropper)

5.4 Normalized Routing Overhead

In this, the ratio of routing overhead is measured through the division between the number of control packet and number of data packets.

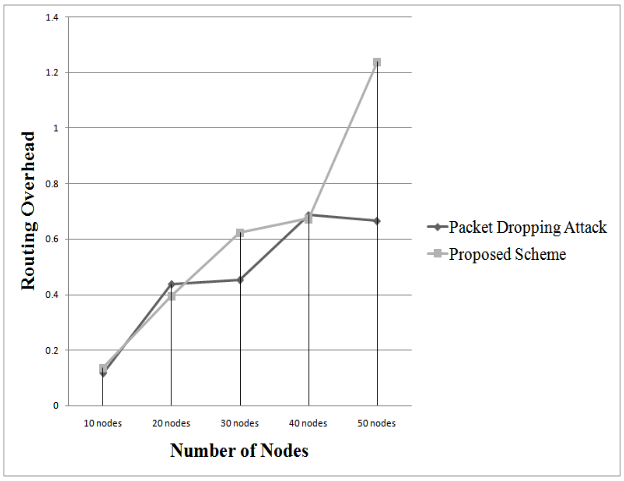


Figure 8: Normalized Routing Overhead (30% Packet Dropper)

5.5 Average Energy Consumption

It measure the average energy that is consumed by mobile nodes during transmission process.

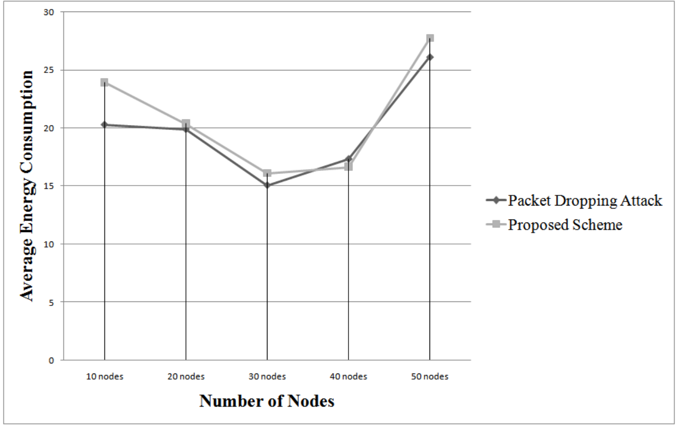


Figure 9: Average Energy Consumption (30% Packet Dropper)

6. CONCLUSION AND FUTURE SCOPE

The effective and efficient field of current research is trust management. In this, paper surveys various trust approaches with their novel conceptions to evaluate route securely. We have figure out that there is no single solution that is feasible to all application and context. Therefore, We have proposed fuzzy system to discover the secure routing by mitigating the packet-dropping attack. The problem of packet dropping attacks in AODV routing protocol is also analyzed in openness network. We have tested out the proposed solution using the NS-2.34 simulator and compared the performance in terms of PDR, E2E Delay, throughput and routing overhead.

In current research, researchers are focusing on TMS where node are behaving equipollently. It means heterogeneity is big issue in wireless network due to higher mobility of nodes. The nodes which have a different capability, security and resources is called heterogeneity. In future, Investigation is needed in terms of highly heterogeneous in the trust evaluation techniques. We will also analyze the results by considering the node's energy efficiency to test out the proposed solution.

7. REFERENCES

[1] Bansal, Meenakshi, Rachna Rajput, and Gaurav Gupta, "Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations", The Internet Society, 1999.

[2] Neetesh Saxena, Narendra S. Chaudhari, “Message Security in Wireless Networks: Infrastructure based vs. Infrastructureless Networks”, IEEE, 2012.

[3] Yu, Shuyao, Youkun Zhang, Chuck Song, and Kai Chen, "A security architecture for mobile ad hoc networks.", In Proceedings of APAN Network Research Workshop, Cairns, Australia, 2003.

[4] Gandhi, Jenish R., and Rutvij H. Jhaveri, "Addressing packet forwarding misbehaviour using trust-based approach in Ad-hoc networks: A survey.", In Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on, IEEE, pp. 391-396, 2015.

Sethi, Srinivas, and Siba K. Udgata, "Fuzzy-based trusted ant routing (FTAR) protocol in mobile ad hoc networks", Multi-disciplinary Trends in Artificial Intelligence, Springer Berlin Heidelberg, Pp. 112-123, 2011.

[6] Marchang, Ningrinla, and Raja Datta, "Light-weight trust-based routing protocol for mobile ad hoc networks", Information Security, IET 6, no. 2, Pp. 77-83, 2012.

[7] Xia, Hui, Zhiping Jia, Xin Li, Lei Ju, and Edwin H-M. Sha, "Trust prediction and trust-based source routing in mobile ad hoc networks", Ad Hoc Networks 11, no. 7, Pp. 2096-2114, 2013.

[8] Bar, Radha Krishna, Jyotsna Kumar Mandal, and Moirangthem Marjit Singh, "QoS of MANet Through Trust based AODV Routing Protocol by Exclusion of Black Hole Attack", Procedia Technology 10, 530-537, 2013.

[9] Biswas, Suparna, Tanumoy Nag, and Sarmistha Neogy, "Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET", In Applications and Innovations in Mobile Computing (AIMoC), IEEE, Pp. 157-164, 2014.

[10] Xia, Hui, Zhiping Jia, and Edwin H-M. Sha, “Research of trust model based on fuzzy theory in mobile ad hoc networks", IET Information Security 8, no. 2, Pp. 88-103, 2013.

[11] Gandhi, Jenish, and Rutvij Jhaveri, "Energy Efficient Routing Approaches in Ad hoc Networks: A Survey.", In Information Systems Design and Intelligent Applications, Springer India, pp. 751-760, 2015.