Asian Journal of Engineering and Applied Technology
ISSN 2249-068X Vol. 7 No. 2, 2018, pp. 74-79

Ensuring the Security by Using Fuzzy Based Trust Routing Scheme in MANET

M. Lalli[1] and J. Lawanya[2]
[1]Assistant Professor, [2]Research Scholar,
School of Computer Science and Engineering, Bharathidasan University, Tiruchirappalli, Tamil Nadu, India
E-Mail: lalli_bdu@yahoo.in

***Abstract*- MANETs are substantially more defenseless to different attacks due to receptiveness in network topology and being endless of a preferred performance in the network. As a result of that, more malicious nodes are regularly intruding without being recognized from the network topology. MANET needs exceptionally particular security techniques to detach the false passage. Also, no single solution is fit into various sorts of the network. The networks perform admirably if the nodes are trusty and act appropriately helpfully. The goal is to enhance the security of the network. This paper begins the new intriguing way to deal with assessing the trustworthiness of the nodes. Fuzzy Trust-based Secured Routing (FTSR) approach presented to deal with a select the trusted route to meet the necessity of the security of the information transmission. In this, the fuzzy logic rule prediction component is adapted to see the future conduct of the node by refreshing the node's trust. We have additionally broken down the execution measurements, for example, the packet transmission rate, end-to-end delay and average throughput which can likewise increment in most up to date approach.**
Keywords: **Mobile Ad Hoc Network, Fuzzy Logic, Fuzzy Trust based Secured Routing, Ad Hoc On-Demand**

I. INTRODUCTION

A self-configuring network design in which distinctive mobile gadgets are connected by remote connection is called MANET [1]. MANET is a less-foundation [2] in which mobile nodes are moving subjective with no administrative division. As a result, the topology may change much of the time at erratic occasions. Mobile gadgets in the ad-hoc network are connected using remote connections. Along these lines, quantifying trust value is the real issue since ad-hoc networks rely upon essential and trust nature of nodes. Because of the quick idea of the nodes, the level of trust additionally changes.

On another side, Security [3] is additionally the primary concern to function the network congruously where the message can be modified through the outsider. As such, we can verbally express that the security issue has been met by accomplishing the accessibility of the network administrations, confidentiality, and respectability of the information. MANETs experiences a few security attacks due to having a few elements, for example, dynamic topology, the absence of focal facilitator, agreeable calculations. Remote connections are significantly more vulnerable to several attacks which makes less demanding for the aggressor to go inside and come outside without being identified. Henceforth, we can verbalize that security of MANETs is the roar of the day. Keeping in mind the end goal to give secure and solid communication and transmission, the analyst needs to get the variants of risk and their impact on MANETs. Moreover, MANETs are open for different threat because communication is based on different nodes which have a mutual trust in one another.

For prosperous communication or transmission, it is obligatory to watch the node's conduct whether a node will partake or not. For this, the paper sets up early approach FTSR which uses fuzzy logic rules. Fuzzy logic is a computational paradigm that constructs an arrangement of client characterized human dialect rules which have converted into scientifically reciprocals to deal with the issue of uncertain and fragmented information. As it were, Fuzzy logic manages rough reasoning instead of settled and correct reasoning. The fuzzy logic may have truth value which has a range in the middle of 0 and 1. The advantage of this framework is adaptability and straightforward.

The current approach maintains the inclusion of misbehaving node during route establishments by using the trust metrics. The FTSR described the misbehaving nodes and trustworthy nodes according to fuzzy levels such as highly trustworthy, trustworthy, untrustworthy, and highly untrustworthy which is represented by the trust values. After getting the nodes trustworthiness, FTSR uses the fuzzy inference rules based on fuzzy levels for secure routing.

II. RELATED WORKS

We have study many research paper [4] from trust management and fuzzy logic. Some of the important papers are defined as below

SrinivasSethi*et al.* [5] proposed FTAR that used Ant-Colony Optimization (ACO). The food-searching algorithm of real ant-agent is called ACO. FTAR is utilizing two parameters, for example, Time-proportion and Dropped packet to classified the stable and malicious nodes. Fuzzification used the time-proportion which is a proportion between the route-answer time and time-to-live. It withal gets to dropped packet parameter used to gauge the number of packet dropped at the node. FTAR uses the ACO by utilizing two kinds of control packet: BANT and FANT.

N.Marchang*et al.* [6] Light-weight means evaluating the trust that one node has for another. In this, each node keeps up the trust anvalue for its neighbor node. The trust value can be habituated to quantify the trust of the neighbor node. For this, each neighbor node contains the three information structures: To Forward, Forwarded, Source list.

Hui Xia *et al.* [7] TSR is the on-demand trust-based unicast routing protocol which is adaptable to locate the ideal route for secure routing. TSR that contains four major phases: Route discovery, Trust application, Trust computation, and Route maintenance. Trust computation contains two procedures: Computation of node's authentic trust and node's present trust. In the node's present trust, the trust estimation of current node position is processed by the fuzzy logic rules prediction technique. Trust application contains three procedures: Route disclosure, Route refresh, and Route handoff process. The protected routing way is picked based on the least trust estimation of the route.

Radha Krishna Bar *et al.* [8] the computation of trust value is relying on two properties, for example, packet sending capacity and weight factor. The weight factor measures through the quantity of RREQ got and through the quantity of RREP sent. After calculation, this trust value is embedded into the routing table, and route disclosure is done based on this trust values as opposed to the traditional shortest path. Amid the route foundation, the less trusted node can be maintained a strategic distance from in AODV routing protocol.SuparnaBiswas*et al.* [9] Trust evaluation of each node is characterized by three parameters: Rank, Remaining battery power, and Stability factor. Rank estimates the dependability of the node. Rank of node drops to 0 characterized the node is an untrusted or malicious node. Remaining battery intensity of a node is considered at a specific time, and Stability factor incorporates two parameters: (I) Pause time (Tpause) and (ii) Velocity for a node is characterized by Vmax.

Hui Xia *et al.* [10] proposed FAPtrust characterize the different trust decision factor based on fuzzy hypothesis. AHP hypothesis based on entropy weight factor used to ascertain the numerous decision factors and use the fuzzy logic prediction rules for register the node's trust value. In this, creator builds up two sorts of trust, to be specific, immediate and circuitous trust. The new approach builds up the trust relationship based on entropy weight technique and fuzzy logic rules prediction component. A fuzzy logic hypothesis is reasonable to characterize the vulnerability and imprecision of the network. In the node's present trust, the trust estimation of the current position of the node is processed by the fuzzy logic rules prediction technique.

III. PROPOSED FUZZY TRUST BASED ROUTING SCHEME

In this section, we presented the change of the selection of the most secure and solid route by building up the trust administration [4] between the nodes. Also, we likewise characterize the fuzzy logic rule prediction strategy to recognize the protected route by segregating the malicious nodes. The steps of the most incipient scheme are defined as below.

Step 1: Before Transmission Process

Step 1.1: In the proposed trust model, each node maintains a trust value forits neighbor node.
Step 1.2: 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 (α + β =1 and α>=0, β<=1)
Let a_1,a_2,a_3...an be the neighbor of node i such that they are also a node of j and n is the number of the neighbor node than trust value can be calculated as,

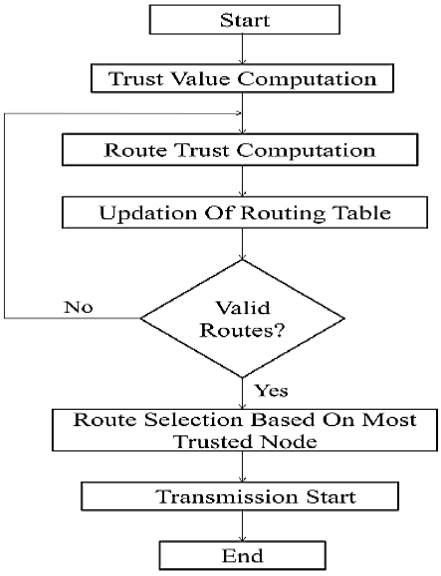

Fig. 1 Before Packet Transmission Process

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

Step 1.3: 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 considered 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

Rr = Ta1(a2) Ta2(a3)… Tal-2(al-1) = Π Tai-2(ai-1)

Step 1.4: For a neighbor node, we have establishes a three data structures: ToForward, Forwarded, and Source List.
To forward: it is utilized to store the number of the packet to be forwarded.
Forwarded: it is utilized to store the number of the packet that is already forwarded.
Source List: it is utilized to define the progenitor of the packet to be forwarded.

*Step 2:*During the packet transmission process

Step 2.1: Promiscuous node maintains the Source List (sc_list) and observes the source of the packet.
Step 2.2: If [(Forwarded) $_{node\ j}$ and (sc_list contains p rogenitor node)]
Step 2.3: (Forwarded) $_{node\ j}$++;
Step 2.4: (ToForward) $_{node\ j}$++;
Step 2.5: If [((Forwarded) $_{node\ j}$>=M or (ToForward) $_{node\ j}$>=M] (CurrentWindow + 1) mod N = 0;
Step 2.6: Else
Step 2.7: Trust Value Calculation

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

Step 2.8: Else
Step 2.9: Promiscuous node fail to update Forwarded, and ToForward count of node j or progenitor node is not in sc_list.

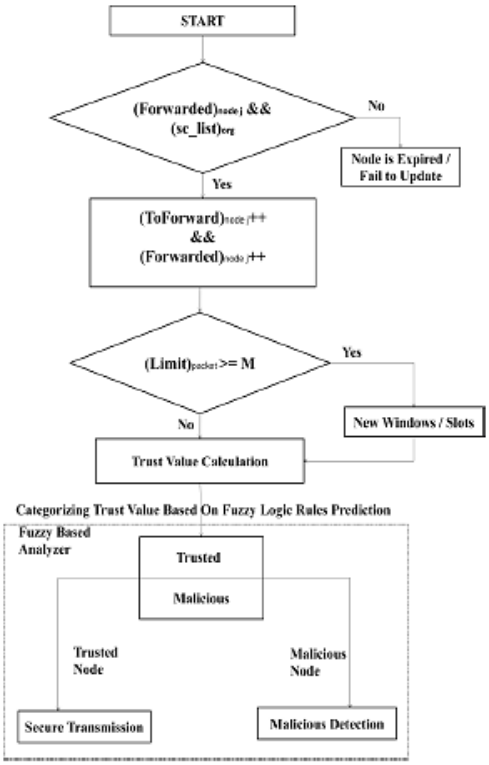

Fig. 2During Packet Transmission Process

*Step 3:*Applying Fuzzy Logic Rules for predicting and observing the current behavior of the malicious node.

Step 3.1: Trust value calculation

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

Step 3.2: Fuzzy Based Analyzer verifies the trust value of the requesting node and performs a lookup in the fuzzy table for the fuzzy trust value. Fuzzy Based Analyzer determines the node as TRUSTED or MALICIOUS.
*Step 3.3:*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.

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

*Step 4:*Applying Fuzzy Logic for foreseeing and watching the future conduct of the malicious node. At the point when node A sends a demand packet to another node B, it is hard for node A to assess whether the node B is ready or not to give benefit. For this,

*Step 4.1:*Consider TV(t) and C(t+1), Where, TV(t): Historical trust an value at t time interval C(t+1): Node's capacity level at t+1 time interim. Node's ability level can be accomplished through giving the administrations, for example, remaining utilization of proportion of battery [11].
Step 4.2: Apply fuzzy operator.

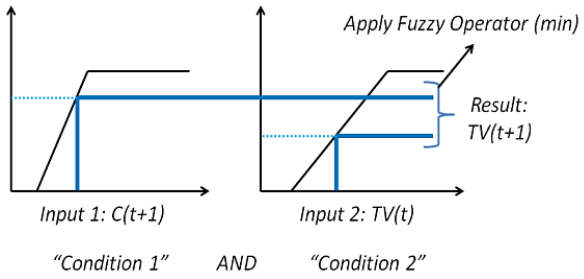

Fig. 3 Fuzzy Operator

Step 4.3: Compare trust value TV(t+1) with a static threshold value.

If (TV(t+1) >= TValue)
Node is Trustworthy
Else
Node is Malicious
Node's trust value will not be refreshed into the routing table, or trusted node will be considered amid the transmission procedure.

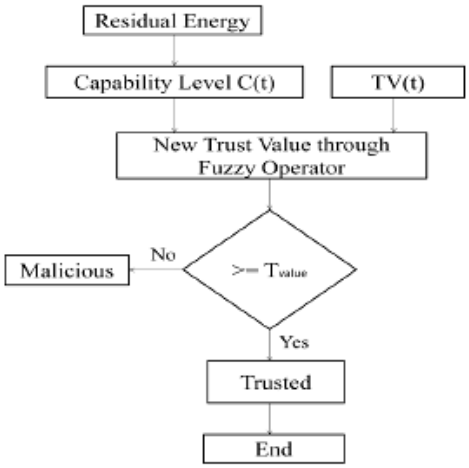

Fig. 4 Future Behavior Observation using Fuzzy Logic Rules Prediction Method

Each above information structures is separated into N openings or windows. Every window or opening the positive whole number value called various packets. The greatest number of packets that every window can store have a settled size number, M. M and N are characterized as configurable parameters. The windows or openings are characterized in a roundabout fashion. We have additionally characterized the CurrentWindow for two information structure which is used to point to the present window or opening in the two information structure. At first, The CurrentWindow can set any number between 0 to N-1.

Construe those indiscriminate nodes happen into the communication. If we consider node I as an unbridled node in the communication, it looked for two sorts of action of node j. Initially, node I look for the packet that is sent to the node j which is to be sent further. Also, secondly, node I look for the packet that is sent by a neighbor of node I to the node j. In this the two cases, at whatever point node I find that node j has gotten the packets which are to be sent more remote than To Forward tally of node j is increased by one. For another situation, at whatever point node finds that node j has sent that packet which is gotten than Forwarded tally is augmented by one. On the off chance that both checks are surpassed the breaking point M than early window will be introduced.

Fuzzy logic gives the capacity to deal with vulnerability and imprecision successfully. Fuzzy logic based calculation for trust has been contrived, and it is connected to the ascertained trust estimation of the nodes. Trust values processed based on Ti (self)(j). These qualities are dealt with as fuzzy information factors, and the Fuzzy logic based calculation denotes the nodes as either trusted or vindictive.

IV. EXPERIMENTAL SETUP

TABLE II SIMULATION PARAMETERS

Simulation time	800 secs
Simulation area	300m × 300m
Number of nodes	600
Frequency of operation	2.4GHz
Node placement	Random
Transmission range	45m
Propagation model	Two-ray
Movement model	Static
Traffic type	CBR (UDP)
Packet size	50 bytes
Packet interval	10 secs
Maximum number of malicious nodes	180
Type of attack	Black hole, on-off attack, conflictingbehavior attack, and bad-mouthing attack
Initial energy	2 Joules

A. Simulation Parameters and Performance Metrics

1. *Packet Loss*. The total number of packet lost honestly or through malicious action with no notification.
2. *Packet Delivery Ratio (PDR)*.The proportion of a total number of packets conveyed to the total number of ion packets sent.
3. *Network Lifetime*. Time taken for the energy of the primary node to fall from 0.5 J to zero and communicated in seconds.

V. RESULT AND DISCUSSION

Figure 5, 6 and 7 depict the performance comparison of the proposed method with another existing method under the packet loss against the different percentage of malicious nodes. Figure 5 gives the packet loss analysis with 10% malicious nodes. Figure 6 depicts the packet loss analysis with 20% malicious nodes and figure 7 gives the packet loss analysis against 30% malicious nodes. Figure 8, figure 9 and figure 10depicts the packet delivery ratio analysis with 10%, 20% and 30% malicious nodes. Figure 8, 9 and 10 give the performance comparison of the packet delivery ratio of the proposed FTRS with other existing methods like 2-ACKT, GTMS, and AODV against the various percentage of malicious nodes. Figure 11, figure 12 and figure 13 depicts the network lifetime analysis with 10%, 20% and 30% malicious nodes. Figure 11,12 and 13 give the performance comparison of network lifetime (secs) using proposed FTRS, 2-ACKT, GTMS and AODV against the percentage of malicious nodes.

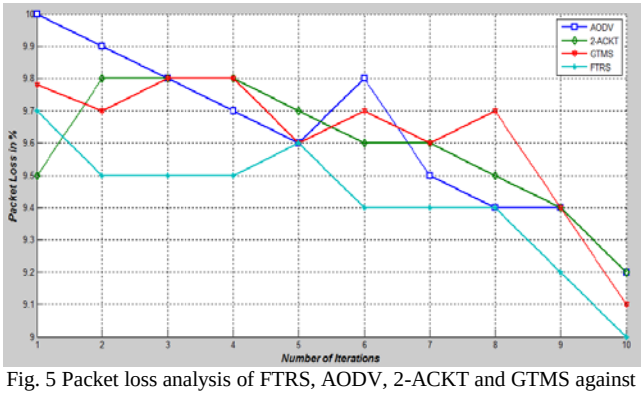

Fig. 5 Packet loss analysis of FTRS, AODV, 2-ACKT and GTMS against some iterations with 10% of malicious nodes

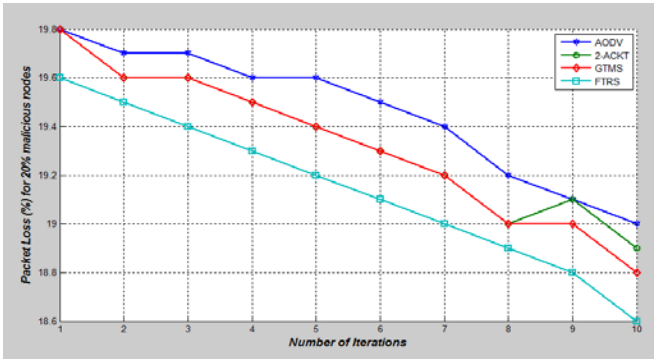

Fig. 6 Packet loss analysis of FTRS, AODV, 2-ACKT and GTMS against some iterations with 20% of malicious nodes

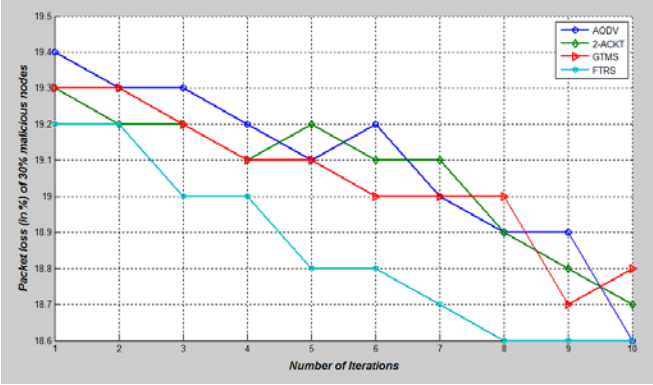

Fig. 7 Packet loss analysis of FTRS, AODV, 2-ACKT and GTMS against some iterations with 30% of malicious nodes

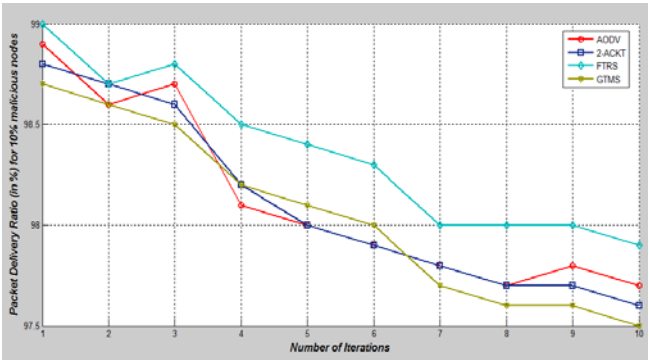

Fig. 8 Packet delivery ratio analysis of FTRS, AODV, 2-ACKT, and GTMS against some iterations with 10% of malicious nodes

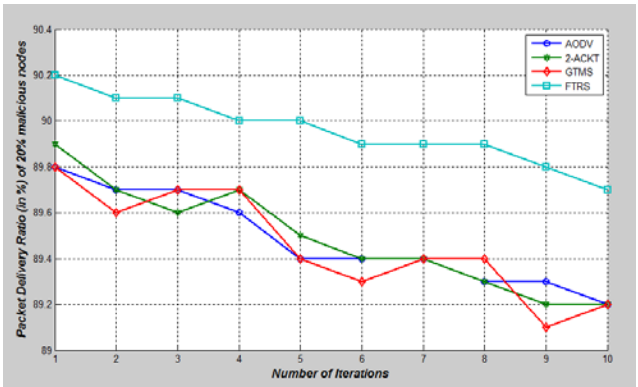

Fig. 9 Packet delivery ratio analysis of FTRS, AODV, 2-ACKT and GTMS against some iterations with 20% of malicious nodes

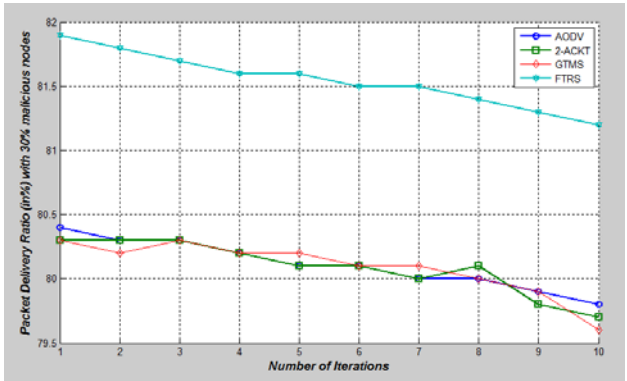

Fig. 10 Packet delivery ratio analysis of FTRS, AODV, 2-ACKT, and GTMS against some iterations with 30% of malicious nodes

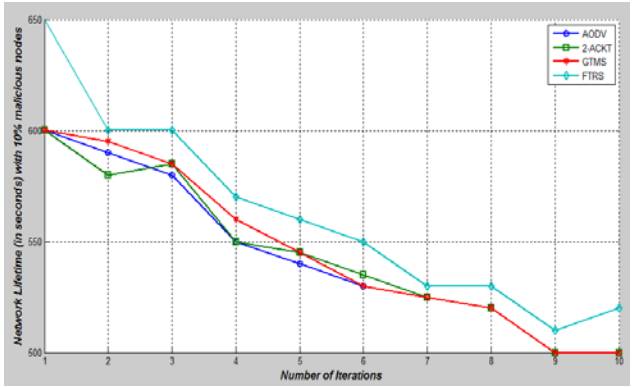

Fig. 11 Network Lifetime analysis of FTRS, AODV, 2-ACKT and GTMS against some iterations with 10% of malicious nodes

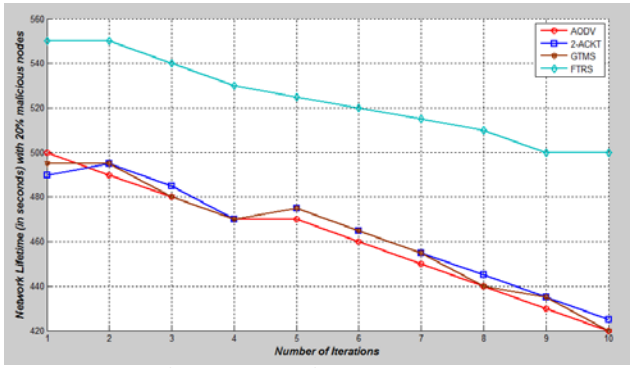

Fig. 12 Network Lifetime analysis of FTRS, AODV, 2-ACKT and GTMS against some iterations with 20% of malicious nodes

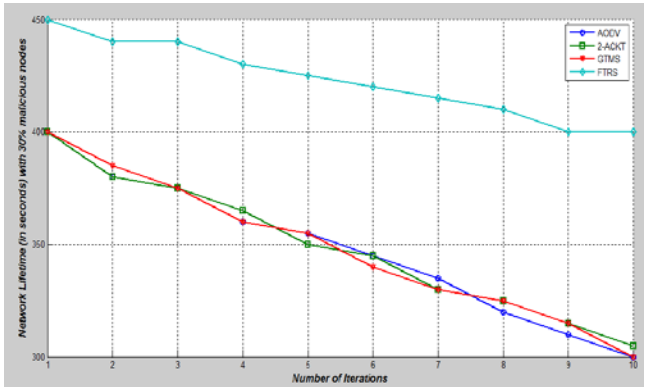

Fig. 13 Network Lifetime analysis of FTRS, AODV, 2-ACKT and GTMS against some iterations with 30% of malicious nodes

From the above figures, it is clear that the proposed method performs well concerning all the performance metrics than the existing methods like 2-ACKT, GTMS, and AODV.

V. CONCLUSION

In this paper, we proposed Fuzzy Trust-based Secured Routing (FTSR) protocol to viably prevent black hole attack, conflicting behavior attack, on-off attack, and bad-mouthing attack. It utilized a fuzzy-based trust prediction model to predict the future direction of a neighboring node based on its historical behavior, trust fluctuations, and recommendation inconsistency. It got from the trust based on the immediate and backhanded observations. It decreases

the energy consumption significantly by avoiding the promiscuous mode of operation for coordinate trust derivation and by gathering assistance only from a subset of neighbors for indirect trust derivation.

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

[5] 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",*IETInformation Security*,Vol. 6, No. 2, pp. 77-83, 2012.

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

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

[9] Biswas, Suparna, Tanumoy Nag and SarmisthaNeogy, "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, ZhipingJia and Edwin H-M. Sha, "Research of trust model based on fuzzy theory in mobile ad hoc networks",*IET Information Security*,Vol. 8, No. 2, pp. 88-103, 2013.

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