International Journal of Security and Its Applications
Vol.9, No.1 (2015), pp.11-24
http://dx.doi.org/10.14257/ijsia.2015.9.1.02

An Enhanced Trust Management Framework for MANET using Fuzzy Prediction Mechanism

V. Hemamalini [1], G. Zayaraz [2] and V. Vijayalakshmi [3]

[1]*Research Scholar, Department of CSE, Pondicherry Engineering College, Puducherry*
[2]*Professor, Department of CSE, Pondicherry Engineering College, Puducherry*
[3]*Assistant Professor, Department of ECE, Pondicherry Engineering College, Puducherry*
[1]*cse.malini@gmail.com,* [2]*zayaraz@pec.edu,* [3]*vijizai@pec.edu*

Abstract

A Mobile Ad hoc Network (MANET) is a self-sufficient arrangement of portable switch and related hosts associated by remote connections. It is a gathering of autonomous versatile hubs that can speak with one another through radio waves. These systems are completely disseminated, and work at wherever without help of any framework. MANETS are substantially more helpless to assault than the wired system. Because of the rapidly changing system topology, versatile hubs frequently comes in and goes out of the system, along these lines permitting any vindictive hub to join the system without being located . Subsequently, Ad Hoc system needs extremely particular security systems. But there is no single approach fitting all the networks, as the nodes can be any devices. Therefore, in this paper, an Enhanced Trust management framework using Adaptive Fuzzy Logic mechanism is proposed to provide detection of malicious node. The proposed model will be incorporated over Ad hoc On-demand Distance Vector (AODV) routing protocol to pick the most limited course that meets the security prerequisites of information bundle transmission. Investigations have been led to assess the productivity and viability of the proposed component in malignant node identification attack resistance.

Keywords: *Manet, Adaptive Trust, Fuzzy Logic, Malicious Node, AODV*

1. Introduction

A mobile ad hoc network (MANET) is an instant infrastructure less wireless mobile nodes that forms a dynamic network without the need for centralized points. As Manet is operated in open environment, it usually suffers from attacks by stingy or malicious nodes, like the packet dropping (black-hole) attack, selective forwarding (gray-hole) on-off attack, bad-mouthing attack, conflict behavior attack so on (Yan Lindsay Sun [8]). Existing security innovations are for the most part focused around encryption and authentication, which are unsatisfactory in the element system topology without a trusted outsider. Additionally, the customary cryptosystem based security instrument is regularly used to oppose the outside assaults. Secure directing is a guaranteeing range for accomplishing better security for the system by securing the steering conventions against malevolent assaults. A few secure directing conventions have been proposed in the writing that was effective in MANET. Then again, Manets are still helpless against different sorts of assaults. Thus, there is a requirement for acquainting a productive system with distinguishes malevolent hubs. Element changes in system's topology cause frail trust relationship among the hubs in the system. In Manet a

ISSN: 1738-9976 IJSIA

versatile hub works as end terminal as well as an intermediate router. Hence, a multi-hop situation happens in Manet, where there may be one or more pernicious nodes in the middle of source and objective. A routing protocol is said to be secure that detects the detrimental effects of malicious nodes in the path from source to destination. Hence trust administration component is thought to be a viable estimation to tackle these issues. There are a few proposed trust administration models under MANET settings, where trust can be considered as the dependence of a system hub on the capacity to forward bundles or offer benefits opportune, essentially and dependably. In this paper, we create another versatile trust administration model for MANET considering the practices of the element hubs in the open network and the entire impacting properties of hubs' dependability. The hubs' trust qualities can be effectively utilized as a part of trust administration procedure, which incorporates the applications like against assault, choice making and so forth. Since a noxious hub carries on in strange ways, this system proposes watching hubs conduct, for example, hubs' versatility, and maintaining a strategic distance from correspondence through these hubs which may prompt more secure directing.

The following work is organized as follows. In Section 2 we discuss the related work. Adaptive trust management model and the calculation of trust value are discussed in Section 3. Section 4 gives the results and discussion and Section 5 gives the concluding remarks.

2. Related Work

The analysis of trust computation is as follows:

2.1. Models of Trust Management

Trust is outlined as the phenomena that the trusting node has the flexibility and capability to deliver a reciprocally in agreement service during a given context and during a given timeslot [7]. It can be expressed as the degree of an associate object or a development which is considered to be true. Using trust management techniques, we can control the security measures of network, which incorporates additionally the quality of cryptographic calculations and choice making authority.

A. A Pirzada [9] presented a model for trust-based communication in ad-hoc networks that demonstrates a central trust authority which identifies malicious nodes. This model presents the thought of conviction and gives an element measure of dependability and reliability in an ad hoc network.

Mui [5] from evolutionism and humanism perspectives initially presented a trust and reputation computing model for generalized systems. In the indirect trust assessment process, they proposed a diagram parallelization calculation, which is instinctive and straightforward.

Based on the work of Mui, Durad *et al.*, [10] introduced a new term: trust of scaling factor that contributed immediate connections and the discernment of suggestion. They likewise proposed an adjusted change calculation.

Using the theory of semi-rings, George [11] proposed a new trust model for ad hoc networks, which depicts trust assessment scheme as a routing path problem in a directed weighted graph. At the point when gathering the conclusion that one element has about an alternate substance, two parallel operations were characterized to assess opinion values from single and various recommendation paths, respectively.

Chang [7] proposed the six characteristics of trust to determine why trust is fuzzy and also proposed a modeling language tool to model the fuzzy. This tool helps to know why trust is dynamic.

Blaze was first to propose the concept of trust management [12], in which authorization delegation was used to resolve the 'stranger' licensing issues. The 'Policy Maker' and 'Keynote' which he proposed bounded the authorization delegation and the public key. Individuals which knew each other's sign authorization certificate based on their trust relationship, the trust was transferred by authorization delegation.

A subjective rationale trust administration model was proposed by Josang [13], which presented the confirmation space and the origination space to portray and measure the idea of trust connections. This model portrayed a set of subjective reason directors for the impelling and sweeping estimation of trust quality. On the other hand, MANET has some default inborn qualities, for example, constrained assets, absence of incorporated devoted server, variable topology, and basic application and so on. As an issue, the approval appointment system and people in general key component are not suitable for MANET, so the conventional trust administration models are not relevant. Thus, in the connection of MANET, there are numerous trust assessment models that have been proposed in the domain of system.

Beth *et al.*, [14] then proposed a trust management model that introduced experience concept to express and measure trust, in which the credibility formula was derived and integrated. This model partitions "trust" into immediate trust and Recommendation trust which were utilized to portray the trust relationship, between the subject and protest, subject and proposal question separately.

Sun *et al*. established a model [15-16], in which trust is measured by entropy. To represent the trust value between two nodes, they introduced an entropy function, which captured the dynamic nature of trust evidence. To figure the roundabout trust esteem, both George and Sun's models considered multi-level coordinated diagram for trust esteem emphasis systems. The convergence speed of this scheme is exponentially slow, when more nodes are involved, and its flexibility becomes a big challenge.

In view of certainty-factor for MANET (CFStrust), Lou and Fan [1] proposed a subjective trust administration display in the wake of considering fuzzy set hypothesis and reputation model, which can be utilized to evaluate and assess the validity of the hubs. Here the issue of trust administration is displayed by fuzzy probability estimation and certainty estimation. The trust assessment system and the determination standards of proposal trust relationship were given in this model. Although two compelling variables relating with mathematical derivations were examined, it didn't consider the hubs' processing power, the shakiness of data transmission through multi-bounces and the attenuation issue of the trust.

Due to rapid expansion of multimedia technology, mobile technology and real time applications, Seema [2] implemented Qos in MANET.

Zapata [4] proposed the Secure Ad hoc On-Demand Distance Vector (SAODV) which is an extension of the AODV routing protocol to protect the route discovery mechanism by providing security features like integrity, authentication and non-repudiation

2.2. Routing Protocols-The Trusted

Traditional routing protocols in ad hoc network may be arranged into 2 essential sorts: proactive and reactive. Proactive routing protocols make and keep up routes all the time keeping in mind the end goal to sidestep the absence of movement all through new route disclosures. Reactive routing protocols find routes only when one hub tries to transmit bundles to an alternate obscure route hub hence on spare assets. The hubs in MANET normally have limited information measure and force vitality; so sensitive routing protocols are the adequate one. Hu, Y. c., Perrig [17], anticipated a reactive single-way routing convention AODV, which blends the destination sequence in DSDV with the on-demand

route discovery technique in DSR. These protocols expect that each one hub is honest and helpful.

Johnson [6] proposed a protocol for routing in ad hoc networks which uses dynamic source routing. This protocol adapts quickly to routing changes when host movement is frequent, yet requires little or no overhead during periods in which hosts move less frequently.

By monitoring the transmission conduct, to assess hub's trust, a few trust-based routing techniques and another class of routing protocols called trusted routing protocols have been proposed by Jensen [18]. These trusted steering conventions comprise of two sections: a trust assessment model and a routing strategy. The selection of next hops or forward paths in a routing strategy is made according to the trust model.

Pirzada *et al.* [3] evaluated the execution of three trust based receptive routing protocols (DSR, trusted AODV, and TORA) by differing the amount of malicious hubs and other experimental settings. The results demonstrate that each trust-based routing protocol has its own particular preference. Specifically, trust-based AODV routing keeps up a stable throughput and surpasses TORA and DSR at higher activity loads.

As another extension to DSR, Guo *et al.* [19] gave a dynamic trust evaluation scheme based on routing model (Trust-DSR). In this model, five route selection systems have been proposed, in view of the trust assessment of the transmission joins. Since its roué selection is restricted on the routes that got from standard DSR, a definitive chose routes is not so much the most believed one.

A fuzzy-based ad hoc on demand distance vector (FAODV) routing protocol was proposed by Manickam *et al.* [20] The authors used fuzzy logic for trust evaluation and a threshold trust value was set up for trust verification. Fuzzy rationale based trust assessment gives a discerning expectation of trust quality and a precise ID of malevolent conduct focused around fuzzy inference rules. Be that as it may, the FAODV display just considers the security strategy against change modification assaults. Furthermore, the trust assessment transform just screens the hub's conduct for route discovery however not for the transmission of information packets.

3. Proposed System

The proposed model computes trust value of each node based on defined decision factors such as direct trust, indirect trust, and energy value aggregation At this point we embrace the Adaptive fuzzy logic rule prediction mechanism that takes verifiable trust esteem as data and figures the current trust estimation of the hub for future choice making interims. The developed trust management model will be incorporated into AODV routing protocol to provide trusted reliable passage delivery route in MANET.QOS will be enhanced while finding route from source to destination in the network. It uses trust qualities to support packet forwarding by keeping up a trust counter table for every hub. When the trust counter range falls below a trust threshold (*i.e.*, ≤ 0.3), the relating intermediate hub is checked as malignant and confined from the system, thereby increasing the performance of the network. Thus the new trust management model developed provides:

i. Improvement in network security
ii. Prevents the network from internal attacks
iii. Guarantees QOS when selecting route from source to destination

The architecture of our proposed system, consists of four major blocks namely,

i. Node Configuration

ii. Trust Computation
    a. Direct factor
    b. Indirect factor
    c. Battery constraints
    d. QoS
iii. Route Discovery & Maintenance
iv. Detection of Malicious node

The detailed description about the architecture is as follows:

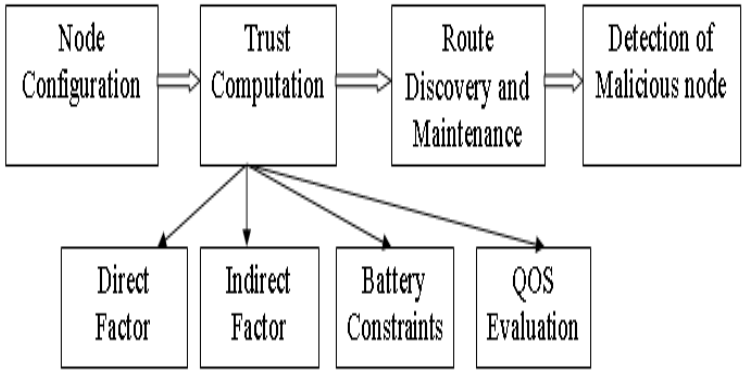

Figure 1. Architecture of Trust Management Model

Figure 1 shows the overall architecture of the proposed work. Route discovery block is nothing but the source routing protocol. Source routing protocol makes routes just when fancied by the source hub. At the point when a hub obliges a route to a destination, it launches a route revelation technique inside the system. This methodology is finished once a route is discovered or all feasible route changes are analyzed. When a route has been built, it is kept up by a route upkeep method till either the destination gets to be unavailable on every way from the supply or till the route is not any more fancied. Trust computation block involves the process of computation of trust value of a node based on the adopted trust model. The node's trusts such as the node's historical trust values and the node's current trust values are computed in this block. By observing a node's behavior the node's historical trust value is computed. The node's current trust is computed based on the historical trust value computed and the node's capability level, using fuzzy logic rule prediction. This two trust value is of great importance and plays a major role in establishing a trusted route to the destination. Trust application block does the procedure of coordinating the trust calculation with the supply routing protocol. During this block, the source routing protocol makes use of the computed node's trust values to ascertain a more reliable and trusted path to the destination. The trusted path is established by the source node to the destination node by satisfying the trust requirement of the system that is nothing but the black-list trust threshold (η). Route maintenance block involves the process of route update. Route update is the process of updating the route from source to destination during the process of data transmission. Due to the mobility nature of the nodes, there is a risk of broken links and alternative routes from the source to destination. Hence route maintenance plays an important role in the process of the trusted source routing protocol.

3.1. Node Configuration

An ad hoc system is constantly involved numerous elements, and every element is a free hub. This segment, shows the model of trust from diagram hypothesis, which is meant as G=<N, L, f >. (i) Trust substance set could be characterized as N= {n1, n2… nk}, where k is the scale of the system; (ii) L is a connection on N, and |L| is the amount of steered system joins. Every l_{ij} in L speaks to a guided edge from hub n_i to its neighbor hub n_j; (3) f: f (l_{ij}) →R∈ [0, 1] means the trust esteem (a genuine number somewhere around 0 and 1) of each one edge l_{ij}. As indicated by definition, the trust model of an ad hoc system could be spoken to as an administered weighted graph.

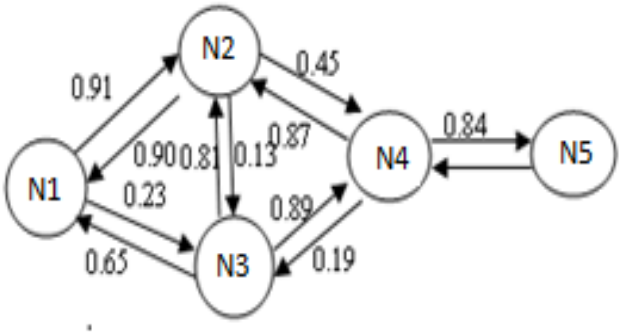

Figure 2. Network Graph for Trust in Ad Hoc Network

In Figure 2, there are five hubs in this ad hoc system. Each one ring speaks to the radiation extent of the relating hub, where the hubs inside the degree are neighbor hubs that can convey straightforwardly.

i) Trust Level of a Node

In this model, TV signifies for a hub's trust esteem, which is characterized in a consistent run somewhere around 0 and 1 (*i.e.* $0 \leq Tn_{ij} \leq 1$). Let n_i and n_j speak to the assessing and assessed hubs, separately. The trust esteem 0 denotes vindictive hub, while the worth 1 intimates complete trust. A basic evaluating rule for trust is characterized, and a case of hub's trust levels is recorded in Table 1. An edge esteem η, termed as the boycott trust limit, is utilized to catch vindictive hubs. As such, if the trust estimation of a hub is more diminutive than η, it will be viewed as a complete doubt hub by its evaluating node.

Table 1. Trust Level of Nodes

Level	Trust Belief	Status
1	[0,η]	Noxious hub
2	[η,0.6]	Less reliable hub
3	[0.6,0.9]	Reliable hub
4	[0.9,1]	Full reliable hub

(ii) Trust Table of a Node

Every hub in the model moreover possesses a trust (Table 2 which relates with Figure 2) with things characterized as takes after:

Table 2. Node N1's Trust Table

Neighbor(Nb)	Tin	Tout	Boycott List
N2	0.90	0.91	No
N3	0.65	0.23	Yes

3.2. Trust Computation

Relationship/Agreement between two neighbor components is defined as 'trust' in an ad hoc network. In this model trust is defined as the dependableness, timeliness, and respectability of message conveyance to their supposed next-hop. Just talking, trust communicates the degree that one hub anticipates that an alternate hub will offer certain administrations. The proposed skeleton assesses trust on a constant scale and considers both hub trust and route trust. In this model, a hub's trust can be considered as an adaptive estimation of the hub's quality of sending, while a route's trust can be utilized to suspect the quality of sending bundles along the route. In general, trust display basically performs trust determination, processing and application. The trust estimation of every hub is processed by utilizing four elements.

- Direct trust
- Recommendation trust
- Energy value aggregation
- Quality of Service

3.2.1. Direct Trust: Two neighbor hubs in a specially appointed system, which can cooperate with one another specifically, secure an immediate trust relationship. If Node a want to calculate the trust value on node b termed as.

$$DiT_{ab} = q_a / q_b$$

Where,
DiT_{ab} is the final direct trust value of a and b.
q_a is the successful packet sent from the node a.
q_b is the successful packet receive from the node b.

3.2.2. Recommendation Trust: The task of indirect trust monitor is to collect or request the trust related information of target node from the neighboring nodes. The neighbor collecting the trust information is another issue. In other words, while requesting the trust information of the target node from neighbors, the direct trust value of that neighbor node should be considered. This is to avoid the security attacks like bad mouthing. This information generally called as Recommendation trust. The recommendation request packet will be broadcasted to all the neighboring nodes from the source node. From the answer packets, fuzzy logic is connected to the immediate trust estimation of all the answered neighbors. The hub with greatest trust worth is considered for assessment of proposal trust esteem. Recommending credibility speaks to the validity level of the suggesting hub (or proposing way) to give proposal experience, which is signified by ReC.

The recommending credibility threshold d_1 is set, if a prescribing hub's recommending credibility is low than this threshold ($ReC<d_1$), the proposal experience given by this hub is not considered. In case if node n_i receives indirect recommendation trust value of node n_j by the intermediate recommendation of node n_m (a single node). By setting, $DiT_{im} = x$, $DiT_{mj} = y$, the recommendation credibility is as follows:

$$ReT^*_{imj} = ReC_{im} \times DiT_{mj} = DiT_{im} \times DiT_{mj} = x * y$$

3.2.3. Energy Value Aggregation: In Mobile Ad hoc system, the hubs are using some vitality for accepting information bundles and some measure of vitality for sending the parcels to neighbor hubs. At first they have greatest vitality that implies hubs with full battery limit. After the correspondence begins vitality utilization additionally begins. This utilization of vitality is more for trusted hubs in light of the fact that, they need to get and in addition send the bundles to its neighbors. In any case in the event of self centered hubs vitality usage is sort of low, they just get information parcels, they won't advance bundles to neighbors. Vitality estimation obliges introductory hub setup that incorporates starting vitality, perfect force utilization, transmission & accepting force utilization. The vitality quality is figured as takes after:

$$Evalue=\rho_{n>0}(\rho_{x=y}E_{Tack}+\rho_{x\neq y}E_{Rack})+\rho_{m>0}(\rho_{x=y}E_{Tack}+\rho_{x\neq y}E_{Rack})$$

Where,
Evalue = vitality used at hub Y because of hub X.
ETack = vitality used for transmission of one acknowledgement (ACK) bundle.
ETpck = vitality used for transmission of one information bundle.
ERack = vitality used for gathering of one ACK bundle.
ERpck = vitality used gathering of one information.

3.2.4. Quality of Service: The Qos necessity of an application is given by a situated of obligations, which might be connection requirements or way demands. A connection obligation tags the confinement on the utilization of connections. A way obligation determines the end-to end Qos necessity on a solitary way. Each one connection in the system is connected with different parameters that could be harshly arranged into added substance and non-added substance stipulations.

Qos directing is "a steering process that sureties to backing to a set of Qos parameters amid making a course". The Qos directing in Manets is required just to backing the interactive media continuous correspondence like feature on-interest, news-on-interest, web searching, explorer data framework and so on. These applications oblige a Qos ensure over a solitary bounce, as well as over the whole remote multi-jump. The Qos directing backings Qos-Driven choice and Qos Reporting and gives way data at every switch.

Table 3. QoS Requirements for Routing Packets

Sl.no	Constraints	Example
1	Additive	Delay
2	Concave	Bandwidth
3	Multiplicative	Loss likelihood
4	Space	System buffer
5	Reliability	Error rate

Factor1: The Qos directing plans can help affirmation control. That is, directing convention not gives course to end, additionally figures the Qos that is supportable on a course amid the methodology of course calculation. It acknowledges another association demand, in the event that it discovers a suitable circle free way from the source to goal having vital assets (transmission capacity) accessible to meet the Qos necessities of craved administrations, generally the association solicitation is rejected.
Factor2: Qos directing plan that considers different demands give better load adjust by dispensing activity on diverse ways subject to the Qos necessities of distinctive traffics. Subsequently the work gives an obvious Qos directing calculation that is versatile, adaptable, and astute enough to settle on a quick choice.

3.3. Node Route Discovery and Maintenance

In route discovery block, the AODV routing protocol creates routes only when desired by the source node. At the point when a hub needs a course to a terminus, it launches a course disclosure system at interims the system. This system is finished once a route is discovered or all possible route changes are analyzed. When a route has been created, it's kept up by a route support method till either the end of the line gets to be out of reach on every way from the supply or till the route isn't any more sought.

Route maintenance is the phenomenon in which a node 'S' is in a position to find a successful path to node 'D', and in case if the topology is being modified suddenly, such that it cannot use its old path to 'D' due to link breakage. Once the route maintenance shows that a supply path is broken, 'S' makes an attempt to use an alternative path it happens to understand to 'D' or invokes a route discovery once more to seek out a brand new route. Route maintenance is employed only if 'S' is truly passing packets to 'D'. A connection split event occasion (such as existed route does not meet the trust requirement of transmitting packets or moving of node) will invoke another trust assessment process and trust route upgrade process.

Additionally, route maintenance guarantees that the route is coordinated and legitimate in a certain time interim (TTL), when a route cache overpowers the most extreme substantial time, and another route revelation will likewise restart. Because of one route disclosure (and additionally through steering information from distinctive packets overhead), a hub may learn and reserve various courses to any end. This permits the response to directing changes to be somewhat speedier, since a hub with various paths to a destination will endeavor an alternate stored route if the one it's been exploitation should fail. This reserving of various routes moreover maintains a strategic distance from the overhead of expecting to perform an alternative disclosure on every event a route being used breaks.

3.4. Detection of Malicious Node

At the point when a hub exists in the boycott list of its whole neighbor's, it will be disposed of in the system. An answer for the issue of element change of a hub's behavior is to punish all the malevolent hubs for a particular time. Every hub in boycott list has a particular duration in which the evaluated hub n_i is viewed as a malevolent hub by the holder (assessing hub n_j) of the boycott list. Amid the particular duration, hub n_i is protected from sending packets and uprooted after the time, from the boycott list and its trust will be set to the boycott list trust edge. Hub n_i will get a chance if hub n_j has a bundle to forward. In the event that the bundle is sent accurately by hub n_i, the trust will increment. On the off chance that the bundle is not sent accurately, hub n_i will be put into the boycott list again and be protected for an alternate term of the particular time. The hub's trust expectation mechanism provides a

MANET with the capacities against a few assaults from malevolent hubs, including black hole and gray hole attack, modification attack, on–off attack, conflict behavior attack, and so on.

4. Results and Discussions

A network model has been created and the results from X-Graph have been taken with the help of NS-2. 50 nodes have been used in this scenario where node ID 0, to node ID 49, is connected to wireless network framing a MANET. Due to battery constraints and dynamically changing network topology the malicious nodes drops the packets. Hence, Enhanced Trust Management model is used to compute the trust value of each node before transmission of packets from source to destination. The Fuzzy Trust based Ad hoc On Demand Distance Vector routing (FTAODV) is used for transmission of packets. The parameters are tabulated in Table 4 as follows:

Table 4. Performance Parameters

Parameter	Value
Simulation time	**300s**
Number of nodes	**50**
Map Size	**1000m**×1000m
Mobility Model	Random Way Point
Traffic type constant bit rate	(CBR)/UDP
Transmission radius	250m
Packet Size	512 bytes
Connection Rate	4pkts/s
Connections	10
Pause Time	2s

The proposed Fuzzy Trust based Ad hoc On Demand Distance Vector routing (FTAODV) is compared with Fuzzy Trust based Dynamic Source Routing (FTDSR), and the results are discussed as follows:

4.1. Delay

It is the time taken by the information bundles from sources to ends, including buffer postponements amid a route disclosure, lining deferrals at interface lines, re-transmission delays at MAC layer and engendering time. As shown in Figure 3 FTAODV has less delay when compared with FTDSR, because FTAODV avoids the malicious nodes thus decreasing the danger of adding delays for resending failed packets.

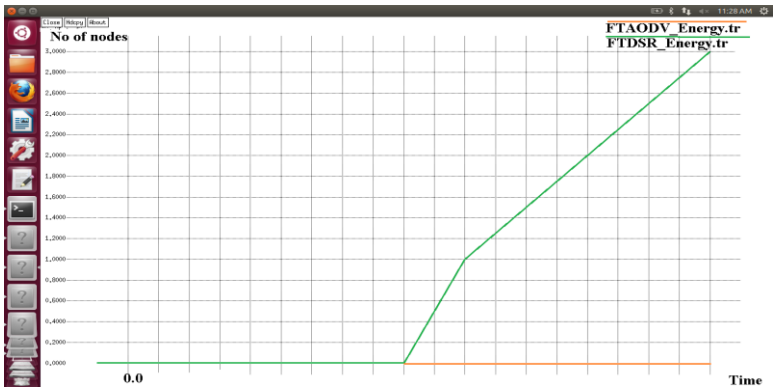

Figure 3. Delay for a Sample of 50 Nodes

4.2. Packet Delivery Ratio

It is the portion of the quantity of information bundles passed on to objective hubs to those sent by source hubs. Figure 4 show that the packet delivery ratio has 90% improvement for FTAODV than FTDSR.

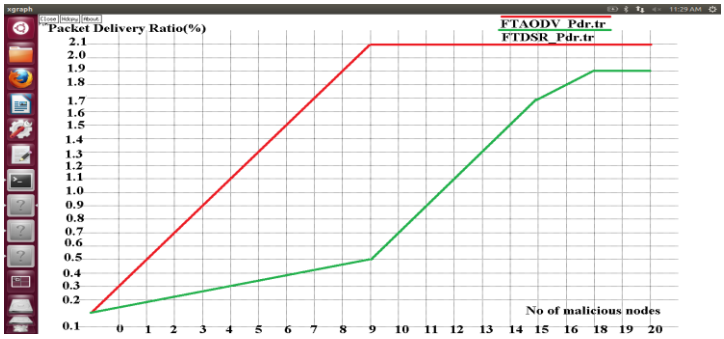

Figure 4. Packet Delivery Ratio for a Sample of 50 Nodes

4.3. Throughput

It is characterized as the measure of advanced information transmitted every unit time from source to end of the line.The throughput for both the protocols are equal for certain time period and then it is seen that the throughput has increased effectively for the FTAODV but for FTDSR, there is only a slight increase in throughput as shown in Figure 5.

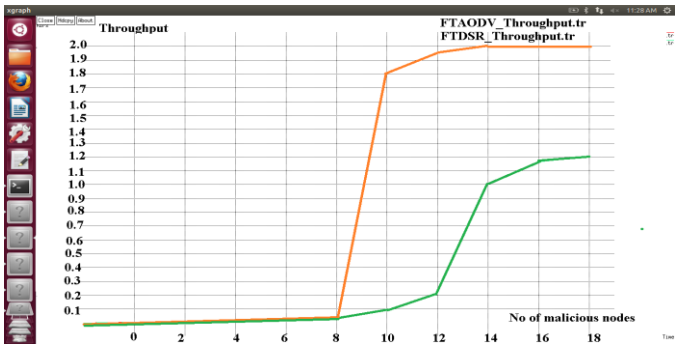

Figure 5. Throughput for a Sample of 50 Nodes

4.4. Routing Packet Overhead

It is the degree of the number of control packets (including route request/reply/ update/error packets) to the number of information packets. Figure 6 shows that routing packet overhead is more for FTDSR than FTAODV.

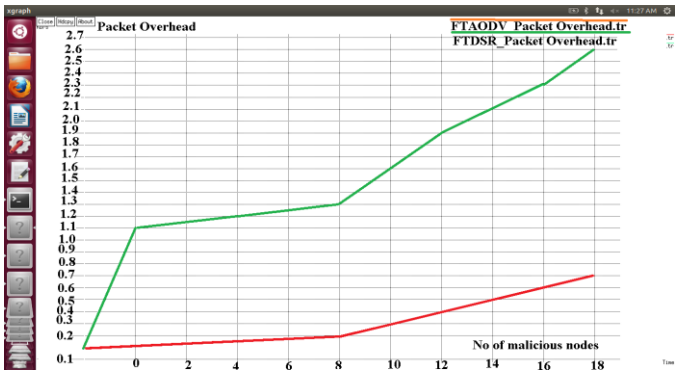

Figure 6. Routing Packet Overhead for a Sample of 50 Nodes

4.5. Energy

The energy level of the nodes in MANET varies due to battery constraints.Hence, if energy level of the node is low then packet dropping will be more.To reduce packet drop,energy of the node is considered for trust computation. Figure 7 shows that the energy level of the nodes is more for FTAODV than FTDSR during transmission of the packets.

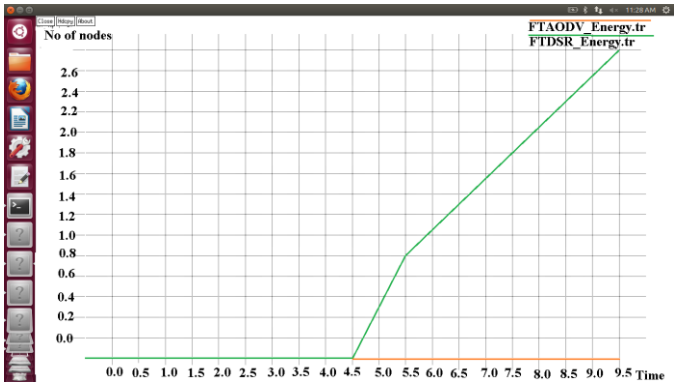

Figure 7. Energy for a Sample of 50 Nodes

5. Conclusion

Based on the inherent characteristics of MANET, an Enhanced Trust management model is proposed to identify malicious nodes in MANET using adaptive fuzzy logic prediction. The developed trust management model is incorporated into AODV routing protocol to provide trusted reliable passage delivery route in MANET.This model shows improvement in packet delivery ratio,delay,throughput and routing packet overhead when compared to Fuzzy Trust based Dynamic Source routing protocol (FTDSR).

References

[1] J. Luo and M. Fan, "A subjective trust management model based on certainty-factor for MANETs", Chinese Journal of Computer Research and Development, vol. 47, no. 3, (**2010**), pp. 515-523.
[2] Seema, Y. Singh and V. Siwach, "Quality of Service in MANET", International Journal of Innovations in Engneering and Technology (IJIET), vol. 1, no. 3, (**2012**) October.
[3] A. A. Pirzada, C. McDonald and A. Datta, "Performance comparison of trust-based reactive routing protocols", IEEE Trans. Mobile Comput., vol. 5, no. 6, (**2006**), pp. 695–710.
[4] M. G. Zapata and N. Asokan, "Secure ad hoc on-demand distance vector routing", ACM Mobile Comput. Commun. Rev., vol. 3, no. 6, (**2002**), pp. 106–107.
[5] L. Mui, "Computational models of trust and reputation: agents, evolutionary games, and social networks", Ph.D. Thesis. MIT. Massachusetts, (**2003**).
[6] D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks", in Tomasz, I., Hank, K. (Eds.): 'Mobile computing' (Kluwer Academic Press, 1996, 1st edn.), pp. 153–181.
[7] E. J. Chang, F. K. Hussain and T. S. Dillon, "Fuzzy nature of trust and dynamic trust modelling in service oriented environments", Proc.Workshop on Secure Web Services, (**2005**) November, pp. 75–83
[8] Y. L. Sun, Z. Han, W. Yu and K. J. R. Liu, "Attacks on trust valuation in distributed networks", Proc. of the 40th Annual Conference on Information Sciences and Systems, (**2006**) March, pp. 1461-1466.
[9] A. A. Pirzada and C. McDonald, "Trust establishment in pure ad-hoc networks", Wireless Personal Communications, vol. 37, (**2006**), pp. 39-168.
[10] M. H. Durad, Y. Cao and L. Zhu, "Two novel trust evaluation algorithms", Proc. of the Communications Circuits and Systems, vol. 3, (**2006)** June, pp. 1641-1646.
[11] George, "Distributed trust evaluation in ad hoc networks", Proc. of the 3rd ACM workshop in Wireless Security, Oct. 2004, pp.1-10.
[12] B. Yu and M. P. Singh, "An evidential model of distributed reputation management", Proc. First Int. Joint Conf. on Autonomous Agents and Multiagent Systems: Part 1, New York, (**2002**), pp. 294–301.
[13] A. Josang, "A logic for uncertain probabilities", Int. J. Uncertainty, Fuzziness, Knowledge-Based Syst., vol. 9, no. 3, (**2001**), pp. 279–31.
[14] T. Beth, M. Borcherding and B. Klein, "Valuation of trust in open network", Proc. ESORICS, (**1994**), pp. 3–18.
[15] Y. L. Sun, W. Yu, Z. Han and L. K. J. Ray, "Information theoretic framework of trust modeling and evaluation for ad hoc networks", IEEE J. Sel. Areas Commun., vol. 24, no. 2, (**2006**), pp. 305–319.
[16] Y. L. Sun, W. Yu, Z. Han and L. K. J. Ray, "Trust modeling and evaluation in ad hoc networks", Proc. Global Telecommunications, (**2005**), pp. 1–10.
[17] Y. C. Hu, A. Perrig and D. B. Johnson, "Ariadne: a secure on-demand routing protocol for ad hoc networks", Proc. Int. Conf. Mobile Computing and Networking (Mobicom'02), Atlanta, Georgia, (**2002**) September, pp. 12–23.
[18] C. D. Jensen and P. O. Connell, "Trust-based route selection in dynamic source routing", Proc. Int. Conf. on Trust Management, Pisa, Italy, (**2006**) May, pp. 150–163.
[19] W. Guo, Z. W. Xiong and Z. T. Li, "Dynamic trust evaluation based routing model for ad hoc networks", Proc. Wireless Communications, Networking and Mobile Computing, vol. 2, (**2005**) September, pp. 727–730.
[20] J. Martin, L. Manickam and S. Shanmugavel, "Fuzzy based trusted ad hoc on-demand distance vector routing protocol for MANET", Adv.Comput. Commun. (ADCOM 2007), (**2007**), pp. 414–421.

Authors

V. Hemamalini, she is currently pursuing Ph.D. in the area of Wireless Security in Pondicherry Engineering College, Puducherry. She completed her B.E from Madras University and M.E from Anna University. She works as Assistant Professor (Sr. G) in Rajiv Gandhi College of Engineering and Technology, Puducherry and has more than 10 years of teaching experience. Her area of specialization includes Computer Networks and Information Security. Email:cse.malini@gmail.com

G. Zayaraz, he is currently working as Professor in Computer Science & Engineering Department at Pondicherry Engineering College, Puducherry, India. He received his Bachelor's, Master's and Doctorate degree in Computer Science & Engineering from Pondicherry University. He has published more than 50 research papers in reputed International Journals and Conferences. His areas of specialization include Software Architecture and Information Security. He is a Reviewer/editorial member for several reputed International Journals and Conferences and Life Member of CSI and ISTE. Email:zayaraz@pec.edu

V. Vijayalakshmi, she is currently working as Assistant Professor in Electronics & Communication Engineering Department at Pondicherry Engineering College, Puducherry, India. She completed her B.Tech, M.Tech and PhD in Pondicherry Engineering College which is affiliated to Pondicherry University. She has 20 years of teaching experience. To her credit, she has published more than 35 research papers relating to Network Security and software Engineering in several National / International Journals and Conferences. Email :vijizai@pec.edu

