Fifth IEEE International Symposium on Embedded Computing

Fuzzy Dynamic Programming based Trusted Routing Decision in Mobile Ad Hoc Networks*

Zhiwei Qin, Zhiping Jia, Xihui Chen
School of Computer Science and Technology, Shandong University,
250101 Shandong, China, E-mail: qzw@mail.sdu.edu.cn

Abstract

In pure mobile ad hoc networks, trust based routing protocol is much more efficient at coping with the dynamic topology, open network environments and works well at identifying malicious behaviors. A number of trust routing protocols proposed restrict at standard routing protocols, therefore, lack accuracy in routing selection and rationality at trust evaluation. In this paper, a novel trust routing decision algorithm based on fuzzy dynamic programming theory has been proposed, which, to the best of our knowledge, is the first such solution proposed. Moreover, we have also proposed a model for trust evaluation and trust update that can be used with our trusted routing protocol. The model is different from other schemes in that it tries to analyze the physical requirements and psychology of the malicious attackers. Extensive simulation has been carried out on verifying the performance of our protocol.

1. Introduction

A mobile ad hoc network is a self-organized multi-hop system comprised by mobile wireless nodes with peer relationships. Two peers out of communication range require intermediate nodes to transfer the messages. Therefore, nodes in a mobile ad hoc network serve as host and router simultaneously. Routing in mobile ad hoc networks faces special challenges when compared to that in the traditional wired networks with fixed infrastructures. Many routing protocols (DSR, AODV, LAR) proposed literally work well in coping with the unstable topology. However, they turn to be inefficient in dealing with the malicious nodes' attacks. Currently, attacks on ad hoc routing mainly come from the exterior networks and the interior nodes. The exterior attacks are always taken by nodes outside the network through injecting erroneous route messages, replaying invalid route messages and so on. The interior attacks are usually caused by internal nodes which have compromised to malicious nodes in the network by behaving badly, abruptly or arbitrarily. For the exterior attacks, encryption is often used [1], however, the solutions require extra management mechanism such as a third party to implement secret key distribution, authentication and data signature et al, which is unsuitable for pure ad hoc networks. For the interior attacks, introducing trust management mechanism based on reputation [2, 3] into routing decision process, can identify and exclude malicious nodes effectively. Trust is defined as the belief that the trusting agent has in the trusted agent's willingness and capability to deliver a mutually agreed service in a given context and in a given timeslot [4, 5]. In mobile ad hoc network, a node requests packet transmission service from its neighbor, the requested node may behave maliciously, which may be induced by selfish, overloaded, malicious thought or be compromised, therefore the requesting node is hard to tell accurately which one is trusted and which one is the most trusted. Considering the fuzzy and dynamic nature of trust and the uncertain factors in routing discovery, based on fuzzy dynamic programming theory, a novel trusted routing model is proposed in this paper. Simulations show that it can accurately identify the malicious nodes and can improve throughput of the network effectively.

The remainder of this paper is organized as follows. Section 2 gives some relevant previous work. In section 3, a trusted routing model in fuzzy environments for mobile ad hoc networks has been established. Then we present the finite horizon trusted routing decision algorithm based on fuzzy dynamic programming and describe the Fuzzy Trusted Dynamic Source Routing (FTDSR) protocol in section 4. Section 5 presents the experiments and analysis on the performance of the protocol. Finally, section 6 concludes the paper.

2. Related works

By monitoring the transmission behavior, evaluating node's reputation, several trust based security routing policy have been proposed.

Sergio Marti et al proposed a Watchdog and Path-rater [6] mechanism based on the DSR protocol. Focusing on the misbehaviors exist on the routing process, Watchdog mechanism in the requesting node firstly monitors the history results of target node's transmission behavior, and then obtains requested node's trust rating. Path-rater then makes a route selection decision according to the ratings. Because the Watchdog mechanism seizes the wireless communication nature of ad hoc networks, and each node can overhear its neighbor's transmission information, the trusting node can accurately capture the malicious behaviors. However, the

*Manuscript received April 2nd, 2008. This work is supported in part by the Natural Science Foundation of China (NSFC) under Grant No. 90718032.

978-0-7695-3348-3/08 $25.00 © 2008 IEEE
DOI 10.1109/SEC.2008.46

watchdog mechanism needs to maintain the state information regarding the monitored nodes and the transmitted packets, which would add a great deal of memory overhead.

As an extension to DSR, Sonja Buchegger et al proposed a new security routing protocol-CONFIDANT [2]. Similarly with the Watchdog Path-rater (WP) mechanism, it firstly introduces a monitor to get trustee's transmission state, with the help of reputation system and trust manager component, it then implements the evaluation and update of the trust rating, which give input to the Path Manager for route decision-making. Different from WP, when computing the monitored node's reputation, the monitoring node always shares information with friend nodes which are defined much more trusted in its own perspectives. Nodes which are identified to be malicious or distrusted will be listed publicly and excluded within a time interval. However, when the time expires, the node will again turn to be a legitimate participant, which may continue its misbehavior. What's more, introducing recommendation trust will make the trust evaluation time-consuming and cause much more overhead, which also increase its complexity. As an extension to DSR, Guo et al [7] gave a dynamic trust evaluation scheme based on routing model (Trust DSR). Five route selection strategies have been proposed, which are based on the trust evaluation of the transmission links. Because its route selection is limited on the routes that obtained from standard DSR, the ultimate selected route is not necessarily the most trusted one.

J.Martin et al [8] proposed a Fuzzy based Ad hoc On-demand Distance Vector (FAODV) Routing Protocol. The authors used Fuzzy Logic at trust evaluation and setup a Threshold Trust Value (*TTV*) for trust verification. Fuzzy Logic based trust evaluation can give a rational prediction of trust value and give an accurate identification of malicious behavior based on fuzzy inference rules. However, the FAODV model only gives the protection method against modification attacks and the trust evaluation process only monitors the node's behavior for route discovery but not for the transmission of data packets. In next section, we will give our trust routing model based on fuzzy dynamic programming.

3. Fuzzy dynamic programming based trust routing model

Traditional routing protocols in ad hoc networks aim at finding a shortest or shorter path from source to the destination. We aim at capturing the characteristic of trusted route and dedicate to accurately and deeply extract the internal root of the misbehavior, make the trusted route selection more flexible and intelligent. In this section we present the trust evaluation model and the trust routing decision-making model.

3.1. Trusted routing model with finite horizon in fuzzy environment

Trust is by nature a fuzzy concept, which poses a fuzzy constraint on the trusted route decision-making. As the goal of a trusted route process is also fuzzy in some sense, we use the fuzzy dynamic programming [9] approach to make a solution in such a fuzzy environment.

Different from traditional routing model in ad hoc networks, we consider the network as a time-invariant finite-state deterministic system under control. Each node is a certain state from the delivered packets' perspective and the transfer between two states can be conceived as two nodes' interaction. The input control variables for each state are the output links with neighbor nodes, then the process of route discovery equals to a multistage state transfer from initial state (source) to terminate (destination) state. In order to model the trusted routing in such environments, we give three basic definitions below:

Definition 1. *State Set* X= $\{\sigma_1,\sigma_2,...,\sigma_{l,}\sigma_{l+1},...,\sigma_n\}$, where σ_i, i=1,2,…n, represents node *i* in an ad hoc network with the scale *n*, it's a finite set.

Definition 2. *Goal Set* T= $\{\sigma_{l+1},...,\sigma_n\}$, which is a specified nonfuzzy subset of X, it represents the destination's neighbor states.

Definition 3. *Input Set* U= $\{\alpha_1,...,\alpha_m\}$, where α_j, j=1,2,…m, equals to *m* links in the network. Because the trust condition of the links is fuzzy by nature, set *U* is a fuzzy set.

Let x_t be the state of the packet being delivered at time *t*, t=0,1,2,…, which ranges over *X*, and let u_t, t=0,1,2,…, be the input control variable at time *t*, which ranges over *U*. Define the temporal evolution of the system to be a state equation:

$$x_{t+1} = f(x_t, u_t) \qquad (1)$$

where t=0,1,2,…, and f is a given fuzzy function from $X \times U$ to X, which means that when the packet at time *t* arrives at state x_t, with the choosey input u_t, then the state will be transferred to state x_{t+1}. Because the input u_t is an alternative from the fuzzy set *U*, and we assume the final goal G is to induce the system state into goal set *T*, so the discovery of trusted route turns out to find an optimal decision D by decision making in a fuzzy environment. We suppose the decision process starts from the initial state σ_1 and ends with σ_n, according to the definition of goal set *T*, the process actually would finish once the system enters *T*, the end time *t* can be given by: $x_t \in T$, with $x_t \notin T$ for $t < N$, where N is the *hop-count*. With the preceding conditions, fuzzy decision is defined as an intersection of the given goals and constraints. Before giving a solution to the problem, we firstly present the fuzzy logic based trust evaluation model for malicious behaviors, which constitutes the fuzzy constraints on input variables in this model.

3.2. Fuzzy logic based trust evaluation model

When the requested node receives a packet transmission request, it's hard to evaluate whether it's willing or not to provide the service. However, the node's capability can be monitored and its history interactions can be recorded, therefore, we can model these factors as follows:

Let C (t) represents the requested node's capability level on providing packets transfer services at time *t*, which includes the remnant utilization ratio of battery, local memory, CPU cycle, and bandwidth at that point. Let H (t) represents at time *t*, its record of history behaviors on offering certain services in the past few time intervals, just like packet-drop ratio. Let TL (t+1) refers to the node's trust level at time *t+1*. Assume the fuzzy member function of C (t) consists of three fuzzy sets-LOW (L), Medial (M) and High (H). The fuzzy membership function of H (t) and TL (t+1) consists of four fuzzy sets-LOW (L), Medial (M), High (H) and VeryHigh (VH) respectively. Combined with social control theory, we give the fuzzy inference rules as follows:

Table 1. Fuzzy rules on trust level TL (*t+1*)

H (*t*) / C (*t*)	L	M	H	VH
L	L			
M	L	M		H
H	L	M	H	VH

The rules in the above table actually establish a mapping from $H \times C$ to TL , which is based on the analysis of the node's current condition and historic behavior. When an overloaded node lacks the CPU cycles, buffer space or available network bandwidth to forward packets, with such a low capability level, even if its historic trust level is very high, it's also untrustworthy in next time interval. This only shows the first rule from above table. Corresponding with each rule, there is an inference relationship R_l :

$$R_l = H_t \times C_t \times TL_{t+1} , \qquad (2)$$

that is for $\forall\ h \in H, c \in C, u \in TL$, we have

$$R_l(h,c,u) = H(h) \wedge C(c) \wedge TL(u) . \qquad (3)$$

For all the *n* rules we have the fuzzy inference relationship

$$R(h,c,u) = \bigvee_{l=1}^{n} R_l(h,c,u) . \qquad (4)$$

For each pair of given input H^*, C^*, using the general total relationship R , we can obtain the output:

$$TL^* = (H^* \times C^*) \circ R , \qquad (5)$$

then with the help of the maximum membership degree approach, we can get explicitly node's trust value $u^* \in [0,1]$ by defuzzification.

3.3. Optimal equation solutions for trusted routing model

Abstracting from a mobile ad hoc networks' characteristics on the topology and wireless communication, we can draw an undirected graph. Considering the model described above, we can obtain the state transfer graph, which can be conceived as a fuzzy system. Figure 1 shows one part of a state transfer graph with 8 nodes.

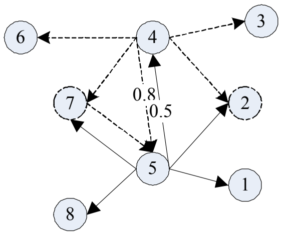

Figure 1. State transfer graph

In the state transfer graph, we need to find a trusted transfer path from initial state *S* to destination *D*. The intermediate states between them can transfer mutually according to the established transfer graph. Take state 4 and state 5 for example, state 4 can be transferred to state 2, 3, 5, 6 and 7, while state 5 can be transferred into state 1, 2, 4, 7 and 8. Moreover, when state 4 is transferred to state 5, it will be constrained by its trust degree on state 5 with the value 0.8, where 0 represents complete distrust, and 1 represents absolute trust in the coming time interval. And when the state transfer process reaches state 4, it will make a decision which state can be its successor under the constraint *C* and the general trust goal *G*. According to the fuzzy dynamic programming theory [10], in such a fuzzy system, for each decision at certain stage, its membership function could get its maximum value. Let $\mu_D^M(\sigma_i)$ denotes the *i* th component of the optimal goal attainment vector, and $\mu_C(\alpha_j \mid \sigma_i)$ is the value of the membership function of the constraint *C* in state σ_i for input α_j , with $\mu_C(\alpha_j \mid \sigma_i)$=1 for *i=l+1,...,n*; and then we can make the decision according to such an equation:

$$\mu_D^M(\sigma_i) = \vee_j (\mu_C(\alpha_j \mid \sigma_i) \wedge \mu_D^M(f(\sigma_i, \alpha_j))) \quad (6)$$

where i =1,2,…n; j=1,2,…m.

According to [10], the author had demonstrated that an optimal policy π must exist in the finite policy space within *l* stages. Modifying from the traditional backward iteration algorithm, we obtain the solution algorithm which is applicable to our model.

4. Trust routing implement

In this section, we will give the trusted routing algorithm based on fuzzy dynamic programming approach, and then describe the process of the trusted route discovery and trusted route maintenance.

4.1. Fuzzy Dynamic Programming based Trust Routing algorithm (FDPTR)

Assumptions: each node in the network maintains a trust table about its neighbor's trust values.

```
Input: each state's trust table $N(\sigma_i)$, $X, T$
Output: optimal policy $\pi(\sigma_1)$ from $\sigma_1$ to $\sigma_n$
$\mu_D^M(\sigma_n) = 1; \mu_D^M(\sigma_m) = 0; m = 1,2,...,n-1.$
t=1; $A = T$;
destination $\sigma_n$ broadcasts optimal goal value $\mu_D^M(\sigma_n)$;
while (t<n)
{for all $\sigma_i \in X$ {
  if ( $\sigma_i$ be triggered && $\mu_D^M(f(\sigma_i,\alpha_j)) \neq 0$ )
  {calculate:
      $\mu_D^M(\sigma_{it}) = \vee_j(\mu_C(\alpha_j \mid \sigma_i) \wedge \mu_D^M(f(\sigma_i,\alpha_j)));$
   if ( $\mu_D^M(\sigma_{it}) <= \mu_D^M(\sigma_{i(t-1)})$ ) delete $\sigma_i$ from A;
   else store: $\pi(\sigma_{it}) = u_i^* = \alpha_j$ , where $\alpha_j$ makes the
   maximum value $\mu_D^M(\sigma_{it})$, in state $\sigma_i$ 's route table; add
   $\sigma_i$ into A;}} /*end if, end for*/
   if (A $\neq \Phi$ ) {
      all the states in A broadcast their corresponding optimal
      goal value; t=t+1; }
   else {
      if ( $\mu_D^M(\sigma_1) == 0$ ) no trusted routing to the state $\sigma_n$ ;
      else
          $\pi(\sigma_1) = (\sigma_1, f(\sigma_1,u_1^*), f(f(\sigma_1,u_1^*),u_2^*),...,\sigma_n);$
      break;}} /*end while*/
return $\pi(\sigma_1)$;
```

Comments: Multistage decision making

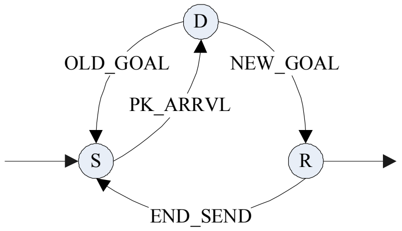

Figure 2. Sub-state transfer graph

The backward iteration process initiates from the destination state. Each state involved in each decision stage besides the destination can be divided into three sub-states. As is shown in figure 2, when the intermediate states receive the ROUTE DECISION (RDE) packet that contains the optimal goal value $\mu_D^M(x_t)$ from the pre-stage states, it will be transferred from Sleep (S) sub-state into Decision (D) sub-state. If the received value is larger than the optimal goal value of pre-stage, the state will enter the Ready (R) sub-state, otherwise it will return to Sleep(S). After a broadcast of the new RDE packet, the Ready(R) sub-state will also turn to Sleep(S), waiting for new arrival RDE packets. Because one state always has several neighbors, a state need to make an iteration decision until obtains the best choice. Take state 4 and state 5 in figure 1 for example, suppose at time *t*, both of them gets their optimal values, then they will broadcast corresponding RDE packets to their neighbor states. States 2 and 7 will receive two RDE packets; moreover, state 4 and 5 will exchange their RDE packets mutually. This may cause two problems:

(1) Time synchronization and asynchronization

In order to avoid the message confliction problem, we adopt the synchronous decision and asynchronous delivery mechanism. At the end time *t* of a stage, all states in set *A* make decisions simultaneously and within certain *time interval* (*TI*) the decision states will broadcast their optimal goal value one after another to its neighbors, a state which receives a RDE packet will wait a certain time *TI* until get enough RDE packets from other neighbor states and then make an integrated decision.

(2) Route cycle problem

In figure 1, suppose state 4's successor is state 7, state 7's successor is 5, then we have $\mu_D^M(4) \geq \mu_D^M(7)$, $\mu_D^M(7) \geq \mu_D^M(5)$, which indicates $\mu_D^M(4) \geq \mu_D^M(5)$. If state 5's successor is 4, we must have $\mu_D^M(5) \geq \mu_D^M(4)$, this condition can work only in the precondition $\mu_D^M(4) = \mu_D^M(5)$, however, according to the algorithm, if $\mu_D^M(4) = \mu_D^M(5)$, the RDE packet will be dropped. So it is unable to form a route cycle. Moreover, the desertion of the packets with equal optimal goal values can decrease the invalid messages in the network and reduce the overhead of network nodes.

4.2. Establish a Fuzzy Trusted Dynamic Source Routing (FTDSR)

Assumptions:

(1) The links between two nodes are bidirectional, this assumption is often valid [11].

(2) Besides the routing table needed in standard DSR protocol, each node in our model additionally owns a trust table with items defined as follows：

N_ID(i) is the identification (ID) of node *i*'s neighbor;

T_IN(i) is the trust value that the neighbor node gets about node *i*;

T_OUT(i) is the trust value that node *i* has about its neighbors. All the trust values are obtained from the trust evaluation model shown in section 3.2.

(3) The packets that contain the trust values are kept from modified by malicious nodes, just like the RDE packet.

Route discovery:

Step 1: Source node *S* initiates a route discovery by broadcasting a ROUTE REQUEST (RRQ) packet that contains the destination address *D* to its' neighbors. The neighbors in turn append their own addresses to the RRQ packet and rebroadcast it. This process continues until a RRQ packet reaches *D*.

Step 2: Terminate node *D* initiates the decision process backwards using the FDPTR algorithm. Current states select next-hop state using the trust table items and store the chosen state in their route tables. After the algorithm finishes, each state obtains its optimal route and the route discovery is implemented.

Route maintenance:

Route maintenance assures the route is integrated and valid in a certain *time interval* (*TI*); a link-broken event will trigger a new trust evaluation process and trust route-update process. Also, when a route table item overwhelms the *maximum valid time*, a new route discovery will also restart.

5. Experiments

In order to verify the correctness of our approach and to see the performance in real application scenario, we establish a pure ad hoc network with 20 nodes distributed over 1000m×1000m area in the simulation platform. The direct radio transmission range of nodes is set to be 250m with the constant speed of 1 m/s, and the simulation continues 100s. We do the simulation three times respectively with three different malicious nodes percentages 12%, 25% and 35%, and each time we compare the performance of our approach with DSR and TDSR [7], during which three metrics are considered.

5.1. Packet drop ratio

The metric of packet drop ratio indicates the selected routing's performance at delivering packets integrally and efficiently. Malicious nodes can take the attack by dropping packets deliberately or forcedly when overloaded. Figure 3 shows the results of the packets drop ratio under DSR, TDSR, and FTDSR protocols respectively.

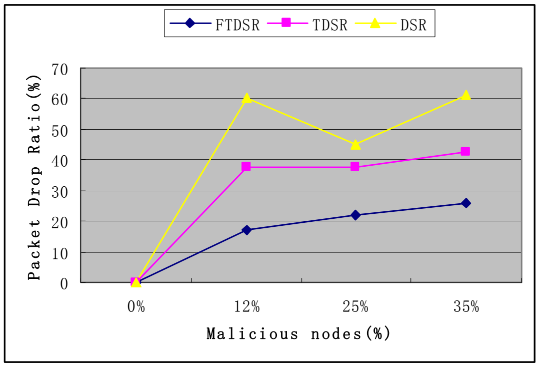

Figure 3. Packet drop ratio plot versus malicious nodes

We can see that FTDSR protocol maintains a lower drop ratio and the curve fluctuates smoother than others. This is because the traditional DSR protocol only considers the hop count as the metric for route selection, the TDSR then chooses the optimal trusted route limited on DSR, while the FTDSR uses a novel method at trust evaluation and route decision, which can eliminate malicious nodes efficiently and mitigate the attack caused by packet-drop. Take 12% malicious nodes for example, the packet drop ratio of FTDSR is 17%, TDSR is 37.5% and DSR is 60%. When the malicious nodes increase from 25% to 35%, the packets dropped by FTDSR increase only 4% while DSR increase 15%.

5.2. End to end delay

The evaluation of End To End Delay (ETE Delay) reflects the mean time in seconds that packets start from source node and reach their respective destination. In order to choose the most trusted path, a backward decision process is implemented which is more complex than DSR and TDSR. What is more, a most trusted route is not always the shortest path, therefore, the end to end latency of FTDSR turns out to be averagely 26% longer than DSR and TDSR. Figure 4 shows the result.

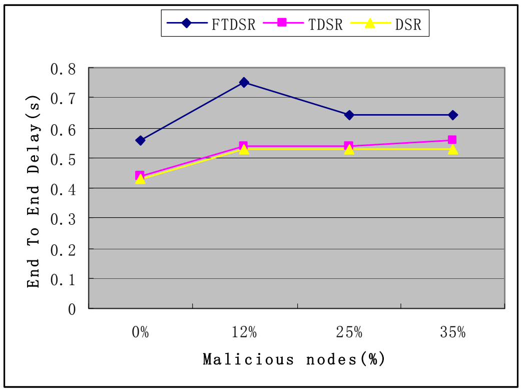

Figure 4. Plot of ETE Delay versus Malicious nodes

5.3. Throughput

Throughput indicates the amount of digital data transmitted per unit time from source to destination.

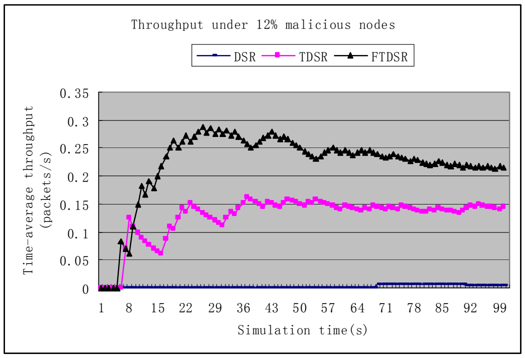

Figure 5. Results under 12% malicious nodes scenario

In order to give an obvious result, we calculate the path's time-average throughput in the destination node which is measured in packets per second. Fig 5, Fig 6, Fig 7 show the throughput of the destination under 12%, 25%, 35% malicious nodes scenario respectively. Comparing the distribution values in each figure, we can see that our approach can always get an obvious higher throughput than DSR and TDSR. Take figure 5 for example, in the end of the simulation, the throughput of TDSR is 0.14 packet per second, and FTDSR is 0.22 packet per second, our approach improves the throughput by 57%.

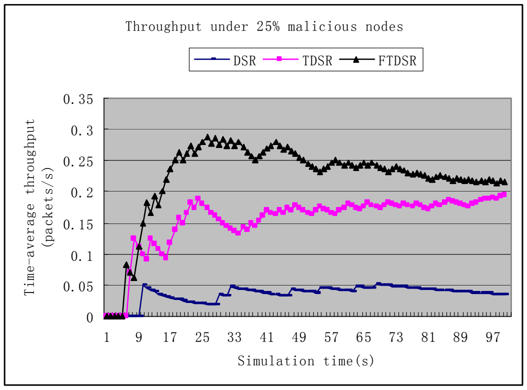

Figure 6. Results under 25% malicious nodes scenario

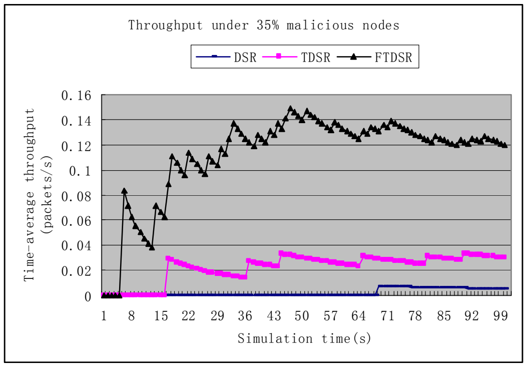

Figure 7. Results under 35% malicious nodes scenario

6. Conclusion

In this paper, a backward fuzzy trusted routing algorithm based on fuzzy dynamic programming approach under mobile ad hoc network environment has been proposed. As a modification to the traditional Dynamic Source Route (DSR) protocol, we have presented a Fuzzy Trust Dynamic Source Route protocol (FTDSR). Compared with the DSR protocol and the TDSR protocol, the simulation shows that FTDSR can accurately purge the malicious nodes and improve the throughput of the network efficiently.

7. References

[1] P. Papadimitratos and Z.J. Haas, "Secure link state routing for mobile ad hoc networks", *Proc. of the IEEE workshop on security and assurance in ad hoc networks*, Jan.2003, pp.379-383.

[2] S. Buchegger and J.-Y Le Boudec, "Performance analysis of the CONFIDANT protocol (Cooperation of nodes: Fairness in dynamic ad hoc networks)", *Proc. of the IEEE/ACM Workshop Mobile Ad Hoc Networking and Computing (MOBIHOC),* June.2002, pp.226-236.

[3] Z. Yan, P. Zhang and T. Virtanen, "Trust evaluation based security solution in ad hoc networks", Available: *http:www.nokia.com/library/files/docs/Trust_Evaluation_Based_Secrity_Solution_in_Ad_Hoc_networks.pdf.*

[4] Elizabeth J. Chang, PFarookh Khadeer Hussain, PTharam S. Dillon, "Fuzzy nature of trust and dynamic trust modeling in service oriented environments", *Proc. of the workshop on Secure web services*, Nov.2005, pp.75-83.

[5] Chang. E, Dillon T, Hussain. F, "Trust and reputation for service oriented environment", *John Wiley and Sons*, 2005.

[6] S. Marti, T.J. Giuli, K. Lai and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", *Proc. of the 6th Annual International Conference on Mobile Computing and Networking*, Aug.2000, pp.255-265.

[7] Guo Wei, Xiong Zhongwei, Li Zhitang, "Dynamic trust evaluation based routing model for ad hoc networks", *Proc. of the Wireless Communications, Networking and Mobile Computing 2005*, Sept.2005, Vol.2, pp.727-730.

[8] Manickam, J. Martin Leo, Shanmugavel. S, "Fuzzy based trusted ad hoc on-demand distance vector routing protocol for MANET", *Advanced Computing and Communications 2007*, Dec.2007, pp.414-421.

[9] Alkan. M, Erkrmen. A.M., Erkmen. l, "Fuzzy dynamic programming", *Proc. of the 7th Mediterranean Eletrotechnical Conference*, Apr.1994, Vol.2, pp.732-726.

[10] R.E. Bellman, L. A. Zadeh, "Decision-Making in a fuzzy environment", *Management Science*, Dec.1970, Vol.17, pp.B141-B164.

[11] Khayata R.E., Puig C.M., Zweig J.M, "A distributed medium access protocol for wireless LANs", *Signals, Systems and Computers 1994*, Nov.1994, Vol.1, pp.238-242.