International Journal of Computer Applications Technology and Research
Volume 3– Issue 6, 333 - 338, 2014, ISSN: 2319–8656

Modeling and Performance Evaluation TAODV Routing Protocol Using Stochastic Petri Nets

Sanaz Talebi
Department of computer science,
Shabestar Branch, Islamic Azad University,
Shabestar, Iran

Mohammad Ali Jabraeil Jamali
Department of computer science,
Shabestar Branch, Islamic Azad University,
Shabestar, Iran

Mehdi Ayar
Department of computer science,
Shabestar Branch, Islamic Azad University,
Shabestar, Iran

Abstract: For a successful route request in Mobile Ad-hoc Networks (MANETs), it is important to know that routing protocols work correctly. On the other hand, this phenomenon acts randomly and it is not often possible to predict their act from one moment to the next. One way for ensuring correct operation of the protocol is to develop a formal model and analyze it. Stochastic Petri Net (SPN) is a formal modeling language which causes the analytical model to be a formal model. Also, prediction of future system's behavior is done in a shorter time than simulation. In this paper, an analytical model based on SPN was presented for TAODV routing protocol. The results showed that the analytical model acted like simulation model in terms of reliability, availability, and mean time to security failure parameters.

Keywords: Mobile Ad-hoc Networks; TAODV routing protocol; Stochastic Petri net; Modeling; Trust

1. INTODUCTION

MANETs are a set of mobile wireless nodes that form a dynamic local network. These networks do not have any central control infrastructure. MANTEs can be formed, integrated together, or divided into separate networks without depending on any fixed infrastructure management. In such networks, each mobile node does not act just as a host but also as a router which sends and transits packets to other mobile nodes if they have overlap in their transition zone [9]. These inherent properties cause MANETs to be more prone to security threats and causes security problems. Because the probability of eavesdropping, spoofing denial of service and impersonation attacks increases, MANETs need to be a trust model. So, trust management in MANETs has made variety applications such as security routing [7]. In development of trust management system in MANETs, the highest focus is on developing secure routing protocols based on trust. One of the proposed routing protocols in this topic is TAODV (Trust AODV).

Considering that simulation is only used to show details of a system, in order to analyze performance of MANET, it cannot do theoretical analysis and predict further behavior of such networks in a large scale and short time. To solve this problem, an analytical model using PNs (Petri Nets) was presented for analyzing performance of a routing protocol. To represent network features using PNs, there are two pre-requisites. 1- A model should be detailed enough to describe some important network characteristics that have significant impact on performance. 2- It should be simple enough to be scalable and analyzable [12]. To show asymptotic behavior of TAODV routing protocol, SPN (Stochastic Petri net) is used. SPN is a way for making an analytical model. It is a directed graph consisting of two parts and is made of two elements of place and transition. It provides time information of a model as exponential distribution and describes dynamic characteristics of the system (concurrency, synchronization, and inconsistency) [6]. PIPE tool [11] is an SPN-based tool. Also, MATLAB software was used to validate and determine accuracy of the proposed analytical model. The rest of this paper is organized as follows. Section 2 is a brief review of the related works. In Section 3, structure of analytical model is presented. Analytical and simulation results are given in Section 4 and conclusions are made in Section 5.

2. RELATED WORKS

According to the numerical analysis and structure of PNs, many works have been done to investigate characteristics such as reliability, availability and so on of wireless network. In [8], an analytical model was presented for AODV and DSR routing protocols using colored Petri Net. In this paper, a topology approximation method was used to solve problem of topology changes. In [4], a key management protocol for GCSs was analyzed to deal with internal and external attacks in MANETs using SPN. In this protocol, a trust chain was introduced. During the analysis, optimal length of a trust chain was calculated. In [3], a mathematical model for quantitatively analyzing a scalable region-based hierarchical group key management protocol was integrated for GCSs in MANETs. In [12], an analytical model was presented for MANETs which made the same results as analytical model. This work is similar to our model.

3. SYSTEM MODEL

In this section, a way is presented for modeling the TAODV routing protocol.

3.1. Analytical Model for Manets Using SPN

According to Table 1, operational area was assumed M * M square meters. Nodes had a radio range equal to R meters and N showed the number of nodes in network. For all the nodes, equal radio range was assumed. The allocated buffer was equal for each node. If the maximum number of received packets of a node was reduced to thresh, the node was converted into node congestion. Max parameter indicated the maximum number received packets of a node. The number of nodes in MANET was assumed constant.

In the presented model using SPN, the store place is created to save all the packets sent by nodes to each other. Figure 1 shows store place and first level of connecting nodes to store place.

Table 1. Assumed values for main parameters

Parameters	Values
M	670m
R	150m
N	4
Packet	512MB
Buffer	2GB
Thresh	1 Packet
Max	4 Packets
Source Node	1
Destination Node	4

In Figure 1, the NODE places show pattern of each node for doing routing protocol. When each of the nodes sends a packet, the OUT transition is fired. Then, the packets are located in the store place. In order to add a new node to the network, a pattern of the node is created and connected to the store place. In SPN, token is used to represent sending and receiving packets. In each node, after packet creation, a copy equal to the number of neighboring nodes is taken and sent to store place, which is shown by weights of the output arc from the OUT transitions. When weight of arc is 3, it means that 3 copies of the packet are sent to the store place. Then, packets are sent to the neighboring nodes.

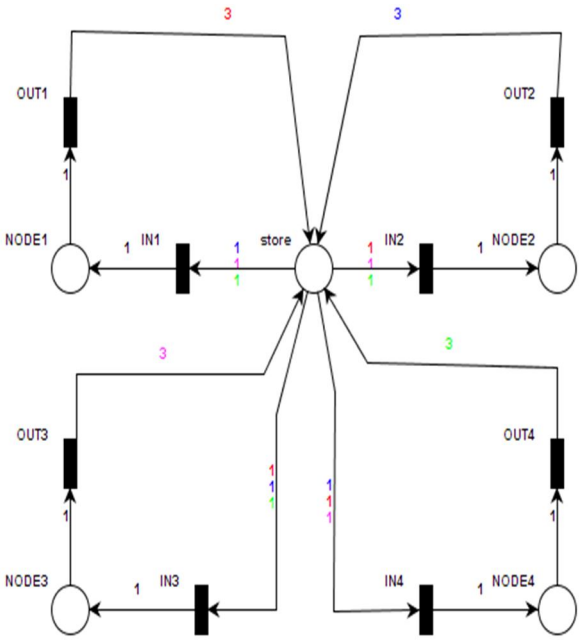

Figure1. Connection nodes to the store place

Figure 2 shows receiving route request packet by a node. For each neighbor node, an arc of the store place is received with 1 weight and the same color with packets of neighbor node.

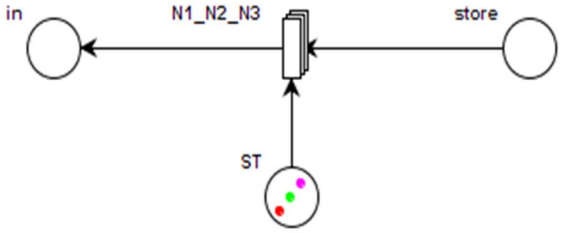

Figure 2. Receiving route request packet by a neighbor node

Because all nodes use the store place, it is possible for a node to receive a packet more than once from a specific node. To avoid this problem, in Figure 2, a place is assumed to be called ST. Initial tokens in the ST place indicate the current node neighbors.

3.2. Analytical Model for TAODV Protocol Using Stochastic Petri Nets

In this analytical model, there are two patterns of nodes in the network: pattern of intermediate nodes and pattern of source and destination nodes. The rest of the paper discusses patterns of nodes.

3.2.1. Intermediate Node's Pattern

There are three types of patterns for receiving packets in intermediate nodes. Intermediate nodes receive the route request packet in order to discover route, the chock packet due to congestion of neighbor nodes and the RREP packet in order to make path. Figure 2 shows receiving the route request packet's pattern and Figure 3 demonstrates receiving the chock packet's pattern by a node. When the RREP packet is generated, if the node is congested, it makes the choke packet and sends to one hop neighbor nodes. Thus, neighbor nodes are notified of the node congestion's condition.

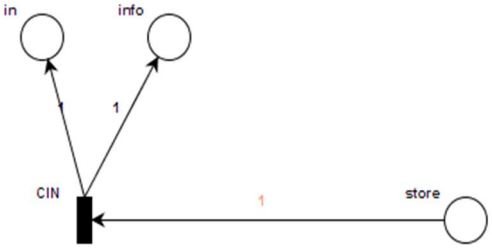

Figure 3. Receiving the chock packet's pattern

In the chock packet's pattern, separate colors are intended for each node. When a node receives the choke packet from the store place, the CIN transition is fired and one token is put in place for processing and allocating a buffer. Also, one token is put in the info place, which shows that a node received the choke packet.

Figure 4 shows the RREP packet's pattern in the intermediate node. In this pattern, when a node received the RREP packet, by firing the REP transition, a token is put in the inc-pen place and one of the inc (the MT1 or the MT2 transition) is fired for calculating penalties or incentives node. The inc transition is for calculating incentive and the MT1 and MT2 transitions are used for calculating penalties. If r> thresh and the sed transition is fired, the RREP packet was sent to the next node. In the route place, the node receiving the RREP packet is specified. The uni place guaranteed that the node will receive the RREP packet just once. When

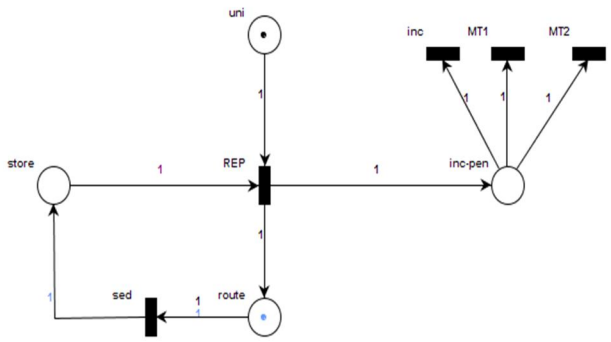

Figure 4. Receiving the RREP packet's pattern

the source node receives the RREP packet, the route discovers the ends.

In Figure 5, when the Ai transition is fired, the packet receives memory from the buffer place. Then, the packet in the WBi place waits for receiving the buffer. An inhibitor arc is necessary from the WBi place to the Ai transition to control the number of input packets. The number of initial tokens in the buffer place indicates the total number of buffer space. If there is a token in the buffer place, the GBi transition is fired, a token is put in the IBi place to process the node, and a token is put in the PM1 place to calculate incentives or penalties. If the input packet is a route request packet, the Te transition is fired. Otherwise, the rec-ch transition is fired to process the choke packet. If the Te transition is fired, it means that the packet is the output packet for the current node. The packet generated by the Ai transition could be deleted in the network. Thus, the received packet from the Te transition was sent to the RBo place for making decisions about sending or deleting the packet. If the rec-ch transition is fired, a token is put in the CH place for receiving the choke packet.

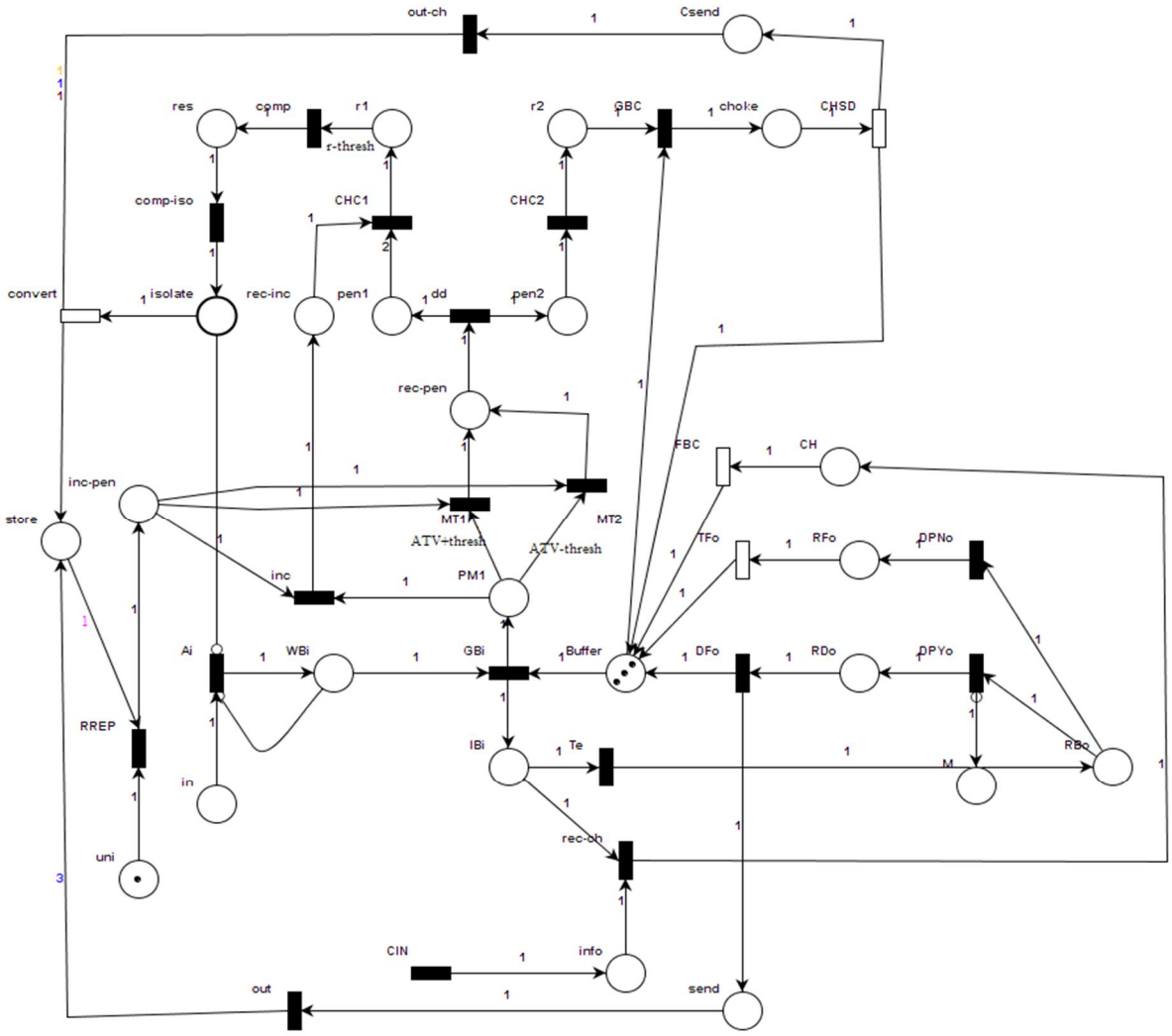

Figure 5. Intermediate node

After ending the choke packet life, the FBC transition is fired and the allocated buffer space is released. The node is congested when the number of receive the RREP packets is outside the node tolerance limit. Otherwise, it will receive incentive. If the node is con-

gested, one of the MT1 and MT2 transitions will happen. Otherwise, one token is placed in the rec-pen place as a penalty and the node is penalized for selfish behavior (no packet is sent to the neighbor node). If none of the MT1 and MT2 transitions are fired, the node will receive incentive.

When a token is placed in the pen2 place as penalty, the CHC2 transition is fired. The presence of a token in the r2 place causes the choke packet to receive the buffer and the choke packet is generated. The CHC1 transition is used to calculate the reduction amount of r parameter (r parameter is the number of packets that a node can receive). For this reason, if the node is not congested, the inc transition is fired and receives incentive. Reduction and multiplicative factors of r parameter are respectively penalties and incentives. For two penalties and one incentive, one token is placed in the r1 place. The comp transition is fired when the number of tokens in the r1 place is equal or more than (r- thresh). In this case, r parameter falls below the thresh parameter. When a token is placed in the isolate place, it does not allow the fire to the Ai transition and the node cannot receive packet until the convert transition is fired.

If there is one token in the RBo place, in the first packet, M place is empty. When the DPYo transition is fired, it puts a token in the RDo place and gets ready to send packet. If the DFo transition is fired, the allocated buffer space is released and a token is placed in the send place. Then, the out transition is fired and the same number of the neighbor nodes makes copy and sends to the store place. If the M place is not empty, the packet is a duplicate packet; so, to delete the packet, the DPNo transition is fired. When a token is placed in the RFo place, the packet gets ready to delete. Firing the TFo transition causes the allocated buffer to get free and the packet to be deleted. When the CHSD transition is fired, one token is put in the Csend place and the choke packet gets ready to send. Then, the out-ch transition is fired and the same number of the neighbor nodes makes copy and sends to the store place.

3.2.2. Source and Destination Node's Pattern

In the source and destination nodes according to Figure 6, the Ao transition is fired as a producer packet and a token is put in the WBo place as a packet. Inhibitor arc is necessary for controlling the number of input packets to the node. With fire the GBo transition, the produced packet receives a buffer and a token is put in the IBo place. Token waits in the IBo place until being put to the RBo place by firing the WTo transition. In this place, there are two cases: first, to send a packet to the neighbor nodes by firing the DPYo transition, the packet gets ready to transfer. In the first

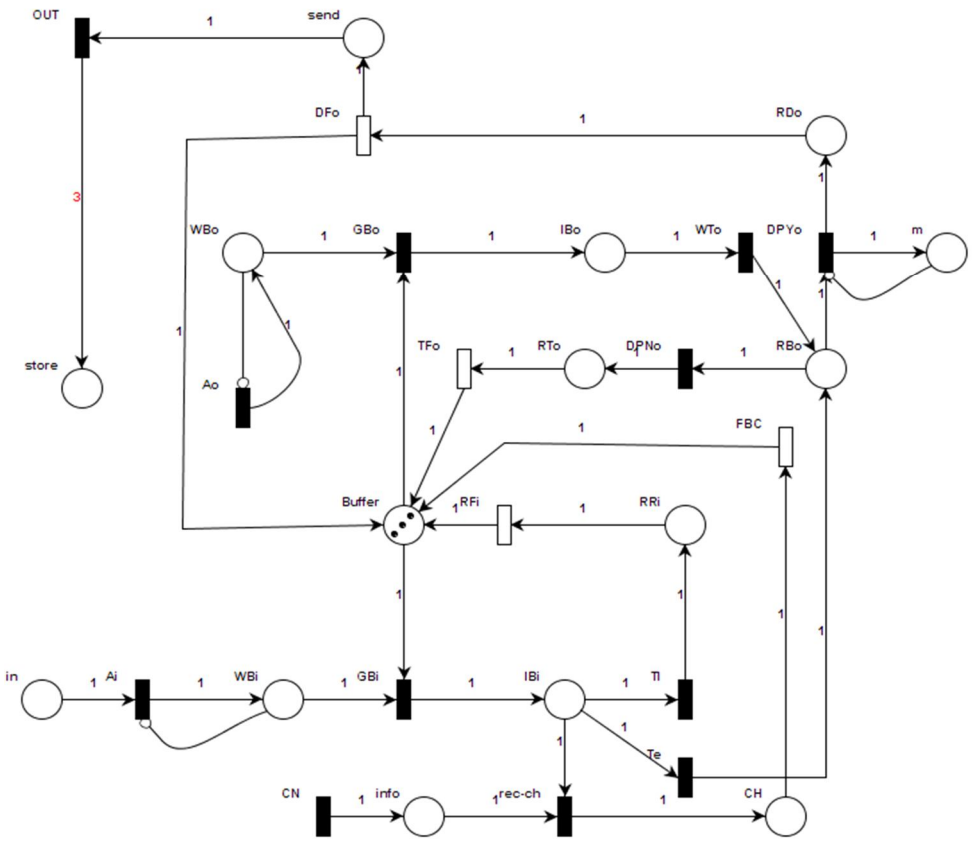

Figure 6. Source and destination node's pattern

time, the packet sends these transition fires. The DFo transition shows start of sending the packet and releasing the buffer. When the OUT transition is fired, the same number of neighbor nodes is put token in the store place. Second, when the DPNo transition is fired, the node gets ready to delete the input packet. The TFo transition shows completion of deleting the packet and releasing the buffer space.

The input packet is entered to current node, when the Ai transition is fired and with inhibitor arc is controlled the number of the input packets. After receiving the buffer and firing the GBi transition, the node will have three cases: first: if the packet should be transmitted to the neighbor node, the Te transition is fired immediately. Second: if the node is the destination node, the Tl transition is fired and a token is put in the RRi place as a received packet. The RFi transition shows completion of the receive packet and releases the allocated buffer space. Third: the input packet is the choke packet; so, the rec-ch transition is fired and a token is put in the CH place. After ending life of the choke packet, the FBC transition is fired and specified space buffer is released to the choke packet. Priority of the transitions is shown in Table 2.

Table 2: Firing priority in intermediate, source and destination nodes

Transitions	Probabilities
rec-ch	3
Te	2
Tl	1
DPNo	1
DPYo	2
MT1	2
MT2	2
MT2	2

4. EVALUATION OF RESULTS

In this section, the designed model is evaluated and compared with the simulation model.

4.1 Evaluation Methods

PIPE tool was used for evaluating the presented model. For validation and comparing the result with the analytical model, MATLAB software was used for simulation.

4.2. Evaluation Criteria

In the following part, the criteria of reliability, availability, and mean time for security failure are introduced.

- Reliability: Reliability in terms of packet delivery rate is a critical factor in the MANETs that evaluates performance of a routing protocol. Packet delivery rate is ratio of number of packets arrived in the destination node to total sent packets from the source node to the destination node [1], [10].
- Availability: To calculate availability, the number of available routes is divided by total number of possible routes [2], [5].
- Security failure: During the following conditions, security failure occurs in the MANETs: 1- if the nodes pretend to congest, 2- more than 1/3 nodes are compromised. In this paper, among the security failure parameters, mean time to security failure (MTTSF) was calculated which showed life time of the network before its arriving at condition of security failure. The high the MTTSF, the later the network's losing integrity or availability.

To calculate the MTTSF in the SPN model, reward allocation method was used so that the reward of 1 was given to all states, except states which will lead to security failure (condition 1 or 2). In each time of receiving reward, a time unit was added to the total time of the network's life time [3].

4.3. The Results of Evaluated

The result of 20 times of simulation by MATLAB software with different topologies was also presented. The nodes were dynamic during the routing. Also, the result of analytical model was presented by PIPE tool with the same topology of simulation environment.

Figure 7 shows rate of packet delivery at the TAODV protocol. On average, packet delivery rate in the simulation was 57% and, based on the proposed analytical model, it was 55%. Usually the simulation result is considered a result; closeness of the result of analytical model to that of simulation model shows that the presented model is accurate.

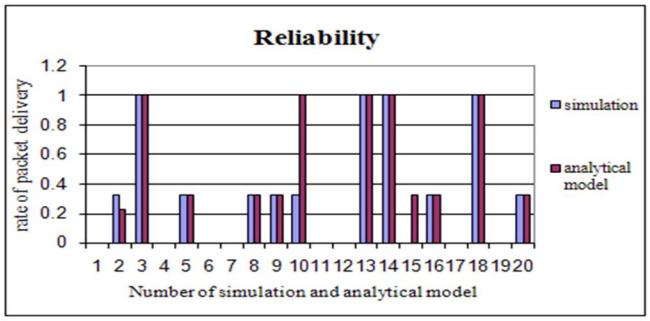

Figure 7. Rate of packet delivery at the TAODV protocol

Availability of simulation and analytical model is shown in Figure 8. The average availability of simulation was 62% and the result of analytical model was 64%.

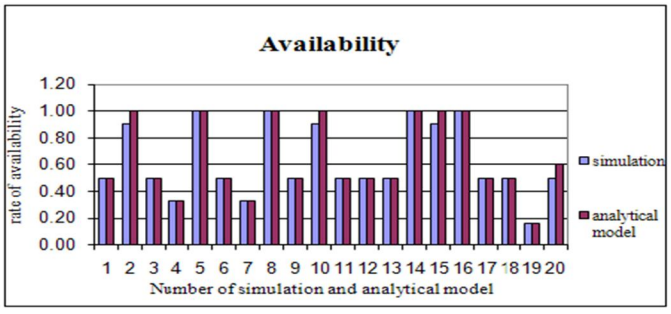

Figure 8. Rate of availability at the TAODV protocol

Figure 9 shows MTTSF in TAODV protocol. In parts that the value was zero, there was not any security failure. Topology of dynamic node showed that analytical model and simulation had different values. In general, in topologies in which there was security failure, the average MTTSF of simulation was 11.6 sec and the average of analytical model was 18.62 sec.

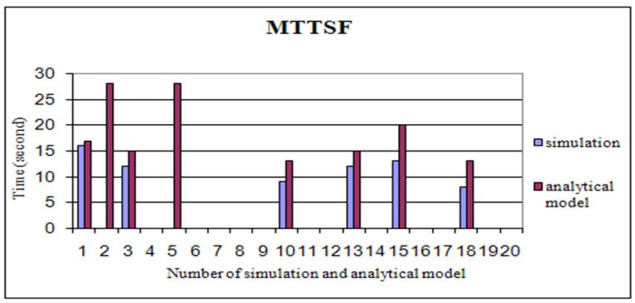

Figure 9. MTTSF in TAODV protocol

5. CONCLUSIONS

In this paper, an analytical model was presented using SPN for TAODV routing protocol. This paper provided a method for analyzing the system properties. This model also presented a theatrical solution while the simulation model presented only details of the system. The obtained results showed that the results of analytical model were close to simulation; so, the proposed analytical model could be a useful alternative for the simulation.

Some properties can be achieved by changing or slightly modifying the model. In this model, all of the time delays were approximated by exponential distributions, which is not always true in a real system. For instance, delays are sometimes constant. As future work, Erlang distributions with a given mean will be applied in the SPN model to approximate the constant distribution, which will increase computational complexity but can improve the presented model with better practicability.

6. REFERENCES

[1] Amandeep, K. G. (2012). Performance Analysis of AODV Routing Protocol in MANETs. *International Journal of Engineering Science and Technology (IJEST).*

[2] Chander K, S. G., Bharat B. (2011). Impact Of Various Factors On Probability Of Reachability In MANETs: A Survey. International journal on applications of graph theory in wireless ad hoc networks and sensor networks(GRAPH-HOC), 3, 12.

[3] Cho J, C. I. (2010). Performance analysis of hierarchical group key management integrated with adaptive intrusion detection in mobile ad hoc networks. Performance Evaluation 68, doi:10.1016/j.peva.2010 .09.005, Published by Elsevier B.V, Journal Homepage: www.elsevier.com/locate/peva

[4] Cho J, S. A., Chen I. (2011). Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks. Journal of Network and Computer Applications, doi:10.1016/j.jnca.2011.03 .016, Published by Elsevier Ltd, Journal Homepage: www.elsevier.com/locate/jnca

[5] Gupta S, K. C., Nagpal C.K, Bhushan B (2012). Performance Evaluation of MANET in Realistic Environment I.J.Modern Education and Computer Science, 2012, 7, 57-64, Published Online July 2012 in MECS Avalable: (http://www.mecs-press.org/) , DOI: 10.5815/ijmecs. .

[6] Haas, P. J. (2002). Stochastic Petri Nets: Modelling, Stability, Simulation: Springer-Verlag New York Berlin Heidelberg.

[7] Omar M, C. Y., Bouabdallah A. (2011). Certification-based trust models in mobile ad hoc networks: A survey and taxonomy. Journal of Network and Computer Applications, *doi:10.1016/j.jnca.2011 .08.008, Available:* *www.elsevier.com/locate/jnca*.

[8] Prasad P, S. B., and Sahoo A. (2009). *Validation of Routing Protocol for Mobile Ad Hoc Networks using Colored Petri Nets* Department of Computer Science and Engineering National Institute of Technology Rourkela

[9] Sarkar S.K, B. T. G., Puttamadappa C. (2007). *Ad Hoc Mobile Wireless Networks, Principles, Protocols, and Applications*: Taylor & Francis Group, New York & London

[10] Sethi S, U. S. K. (2010). Optimized and Reliable AODV for MANET *International Journal of Computer Applications (0975 – 8887) 3.*

[11] tools, P. from http://pipe2.sourcefroge.net/

[12] Zhang CO, Z. M. (2003). A Stochastic Petri Net Approach to Modeling and Analysis of Ad Hoc Network *NJ, 07102*