


ITC 4/49 Information Technology and Control Vol. 49 / No. 4 / 2020 pp. 556-563 DOI 10.5755/j01.itc.49.4.25438	Trusted Sensing Model for Mobile Ad HoC Network Using Differential Evolution Algorithm	
	Received 2020/03/05	Accepted after revision 2020/10/06
	 http://dx.doi.org/10.5755/j01.itc.49.4.25438	

HOW TO CITE: Elamparithi, P., Ruba Soundar, K. (2020). Trusted Sensing Model for Mobile Ad HoC Network Using Differential Evolution Algorithm. *Information Technology and Control*, 49(4), 556-563. <https://doi.org/10.5755/j01.itc.49.4.25438>

Trusted Sensing Model for Mobile Ad HoC Network Using Differential Evolution Algorithm

P. Elamparithi

Department of CSE; AAA College of Engineering & Technology; Sivakasi, India;
e-mail: elamparithi@aaacet.ac.in

K. Ruba Soundar

Department of CSE; P.S.R Engineering College; Sivakasi, India; e-mail: rubasoundar@psr.edu.in

Corresponding author: elamparithi@aaacet.ac.in

Mobile Ad Hoc Network (MANET) has a set of mobile nodes that are allowed to communicate with each other through wireless links. The nodes are deployed spontaneously without any infrastructure in a geographical area. Due to the lack of centralized administration and prior organization, MANETs are vulnerable to different attacks of malicious nodes. To overcome the problem of black hole attack in MANETs, a trust model using Differential Evolution (DE) algorithm has been proposed. It identifies the malicious node and inhibits them to become the member of data transmission path. The proposed work consists of two phases; one is to obtain the optimized path and the other deals with the penalty factor for malicious nodes. Moreover, the Differential Evolution is one of the most promising optimization to enhance security with increased network density. The proposed algorithm is compared with Ad Hoc on Demand Multipath Distance Vector (AOMDV), Dynamic Source Routing (DSR), Genetic algorithm and Ant Colony Optimization (ACO).

KEYWORDS: Trust Model, Differential Evolution, Penalty factor, Fitness function, Black hole attack.

1. Introduction

The mobile Ad Hoc Network facilitate wireless network without any centralized unit and it involves participation of all the nodes in the network in an honest manner. Because of the dynamic nature and lack of centralized unit, the network is vulnerable to various types of attacks by malicious node. Hence, the security of the MANET can be enhanced by considering the trust value of the node. Few attackers create network position such as worm hole attack and fake functional routes by injecting false route information externally. Other attacks like a black hole, gray hole attack, modification and sybil attack are caused by imprecise routing information. The malicious node affects the legitimate node to alter the information flow in the network. These attacks are challenging and are due to the mobility of the node which results in dynamic topology.

The proposed work deals with the black hole attack, which is an advertisement of the metrics made by attacker to all nearby nodes or destination. Thus, the malicious node creates false routing information, asserting that it has an optimal route which causes other normal nodes to route data packets through the one which is malicious. Every packet that it receives is therefore dropped instead of forwarding those packets normally. This attack causes abnormal delivery of the packets and the trustworthiness of the nodes plays a major role here.

The security of the network can be greatly improved by considering the trustworthiness of other nodes in the network without considering the centralized unit. In a trusted environment, to detect the presence of malicious nodes, the trust level of other nodes in the network plays a major role. By this mechanism, the nodes are capable of deciding to which extent the nodes can be trusted for further communication. The nodes with low trust value are kept away and are not included in the communication. Similarly, the proposed trusted sensing model ensures secured data transmission by calculating optimized path and trust update mechanism. The differential evolution algorithm opts for the best optimized path based on the distrust factor. The proposed fitness function search for all feasible paths and obtains the best solution. The trust update mechanism identifies the packet dropping (malicious activity) and deals with the penalty factor by taking into account the previous and the current trust value of the node. As in

[10], DE algorithm has four steps, such as initialization, mutation, crossover and selection. These steps are repeated until the termination condition is met and the two control parameters 'F and Cr' are kept constant. Hence, the designed model reduces the distrust factor and improves the reliability of the path.

The remaining paper is arranged in the following sections; Section 2 discusses the literature related to the related value and Differential Evolution algorithm. The proposed trust sensing model is discussed in Section 3; Section 4 discusses the experimentation of simulation results and the conclusion of the proposed work is represented in Section 5.

2. Related Work

In the scientific literature, the studies reveal that, only a few researchers have worked on DE – based trust calculation to handle the issues in mobile Ad Hoc Network. Most of the Differential Evolution algorithm concentrates in optimal path selection, topology control maintenance and routing protocol. In MANET, the multicast routing problem is resolved using multi objective differential evolution algorithm [14] which converges faster. Here, the crossover and mutation operators are modified to build the shortest path to improve the network lifetime and bandwidth of the network. This motivated to use the differential evolution algorithm to identify black hole attack in MANET with different mutation strategies. DE has various mutation strategies as the authors in [4] selected DE/best/1 to select the cluster head for clustering. Other mutation strategy DE/rand/1 is used to select the optimal path in the wireless sensor network as in [2, 18]. In the topology control mechanism [7, 6], the DE/rand/1/bin mutation strategy is used for the placement of sensor nodes and maintenance of connective nodes respectively. For the optimal path selection using GA, flipping based mutation strategy is used as discussed [1, 9]. The mutation variants are changed according to the application. The hybrid method differential evolution with nature inspired firefly algorithm in [3] obtains optimal feasible path for the network where the objective function satisfies the QoS constraints in the MANETs.

For security based applications in mobile Ad Hoc Network, the trust plays a major role to establish secure communication. The trust values reveal the truthfulness of the target nodes future behavior. In addition, it acts as a defensive mechanism against the misbehaving target node and is of two types as direct trust and indirect trust. Further, the computation of trust is carried out in two ways [5] as centralized approach and distributed approach. A central node called agent computes the trust of the node in the centralized techniques, whereas, in distributed computation, the node calculates its own trust based on the neighbor node behavior. The trust prediction model [16] predicts the secured route and identifies the malicious activity by computing trust computation for the past node activity. The network intrusion threat detection in [13] is based on the probabilistic neural network model and it secures the network from both the internal and external malicious attack. The system uses hybrid model that integrates principal component analysis and probabilistic neural network for detecting the network intrusion data. Few trust model strategies with their trust schemes are discussed in Table 1.

Table 1

Trust Models and Trust Schemes

Method	Trust Values	Attacks
Minimize the uncertainty in both reactive and proactive protocols [12] based on the mobility factor	Belief, Disbelief and Uncertainty	Identifies misbehaving nodes
Trust model based on fuzzy logic [16] under routing constraints	Historical trust, Current trust and Route trust	Identifies black hole attack and the malicious node to obtain optimal routes
Handles uncertainty using trust value and punishment factor [15] to enrich the network security	Direct trust and Indirect trust	Identifies malicious nodes
Trust aging factor [11] to improve network lifetime	Direct trust and Indirect trust	Identifies a malicious node and selfish node
Gray - Markov chain model to predict the node's trust level [17]	Trust (Subjective reputation) and Indirect reputation	Identifies a malicious node

By considering all these factors, the proposed work uses direct trust alone. The main contributions of the research work include

- Designing of the trust sensing model using the differential evolution algorithm with best mutation strategy.
- Obtaining optimized shortest path using minimized fitness function of distrust factor and trust formulation based on direct observations.
- Trust update function using the penalty factor to influence the malicious node and inhibit to be a part of best fit path.

3. Trust Sensing Model Using DE Algorithm

The proposed algorithm / model ensures a trusted path by eliminating the black hole attack, which effectively improves the performance of the network. The trust value is used in building the secure path which induces the malicious node to participate in the optimization of routes. The main components of the trust sensing model are the optimized path model and trust updating model.

3.1. Optimized Path Model

The mobile ad hoc network is considered as a graph $G = (V, E)$ where V represents the vertex and E is the set of links that exist between the vertexes. All the possible existing paths are coded as the structure of the chromosome where the initial and final genes are assigned for source node and the destination node. Since there is a number of intermediate nodes in all the paths, the length of the chromosome variants and the main condition is that the particular node in the network can participate only once. The trust of the node is calculated only when there is a link between the nodes. It is represented by a symmetric matrix which has all the information about the links in the network at time 't' and is represented as L_{AB} .

$$L_{AB} = \begin{cases} 1 * Trust_{AB}, & \text{if link exists} \\ 0, & \text{otherwise,} \end{cases} \quad (1)$$

where $Trust_{AB}$ is the trust of node A on node B. Each and every node maintains the trust value information

of its own for other neighbor nodes. Due to the mobility in the network, the node A is capable of moving away from node B where no link exists between them. Hence, no trust evaluation is required because the proposed trust sensing model considers the direct trust evaluation alone.

3.2. Trust Formulation

The trust formulation of trust is the ratio of successful forwarded packet (P)_F to the total number of packets to be forwarded (P)_{TF} as shown in Equation 2.

$$Trust_{AB} = \frac{(P)_F}{(P)_{TF}}, \tag{2}$$

where, Trust_{AB} - Trust value of node A on node B, (P)_F - Total number of packets forwarded (success), (P)_{TF} - Total packet to be forwarded

Furthermore, the trust value generated by means of interaction between the two nodes defines trust propagation and is formulated as in Equation 3.

$$nTrust_{AB} = w_1 * D_{A,B} + w_2 * C_{A,B}, \tag{3}$$

where w_1 and w_2 are the weights assigned to trust ratio of the data packet and control packet, respectively. Therefore, the weights are represented as $w_1, w_2 = (1-w_1) \geq 0$.

3.3. Formulation of Fitness Function

In order to find the secured path and identify the black hole attack causing malicious node, the fitness function is therefore mapped with the distrust factor. The distrust factor is shown in Equation 4.

$$\overline{nTrust_{AB}} = 1 - nTrust_{AB} \tag{4}$$

Here, $\overline{nTrust_{A,B}}$ is the distrust factor created by Node A on Node B. As the Differential Evolution algorithm deals with the minimization factor, the distrust value is considered for evaluation, which means that node with high trust value is assured. The fitness function is defined as

$$Minimize f = \sum_{\substack{DN=A \\ SN=B \\ A \in IN}}^{DN-1} \overline{nTrust_{AB}} + \Delta T * \tau, \tag{5}$$

Here ΔT is an additional trust threshold which influences the malicious node, τ is the hop count and $\overline{nTrust_{A,B}}$ is the distrust factor between node A and node B. Additionally, the term “IN” denotes the Intermediate Node set between the Source Node (SN) and the Destination Node (DN).

3.4. Update of Trust Value

The trust value of the node changes dynamically on every iteration. The trust updation involves the combination of current trust of a node and its previous value of trust. It is based on the effect of the black hole attack caused by malicious node where there will be more packet dropping. Hence, the trust updation is based on two situations as,

- 1 presence of packet dropping (malicious activity) and/or
- 2 no malicious activity

Scenario 1: Fluctuation in trust value because of the presence of packet dropping

$$Trust_{AB}^{New} = \begin{cases} \psi Trust_{AB}^{old} + (1-\psi)Trust_{AB}^{cur} * (1-\rho), & \text{if } (P_f \leq P_s) \\ \psi Trust_{AB}^{old} + (1-\psi)Trust_{AB}^{cur} * \left(\frac{1-\rho}{1+\rho}\right), & \text{if } (P_f > P_s) \\ \psi Trust_{AB}^{old}, & \text{if } (Trust_{AB}^{cur} = 0) \wedge (P_s = 0), \end{cases} \tag{6}$$

Scenario 2: Current Trust ($Trust_{AB}^{cur} = 1$) with no malicious activity

$$Trust_{AB}^{new} = \psi Trust_{AB}^{old} + (1-\psi)Trust_{AB}^{cur}, \text{ if } Trust_{AB}^{cur} = 1, \tag{7}$$

Here, $Trust_{AB}^{new}$ - New updated trust of node A and node B, $Trust_{AB}^{old}$ - Old trust value of node A and node B, $Trust_{AB}^{cur}$ - Current trust value of node A and node B, ψ - Trust equivalence factor ranges from 0 to 1, P_s - Successful packets count, P_f - Failure packets count, ρ - Penalty factor ratio.

The penalty factor ratio (ρ) is defined as the ratio of failure packets to the successful packets delivered as shown in Equation 8.

$$\rho = \frac{P_f}{P_s}. \tag{8}$$

This penalty factor affects the trust value of the node whenever packet dropping occurs and, thereby, it is

observed that when the trust value of the node goes below the threshold limit, that particular node will be blocked in its list. Each and every node in the ad hoc network maintains a separate trust table and updates the trust value at a particular time interval.

3.5. Differential Evolution Algorithm

In the differential evolution algorithm, let the initial population be expressed as P_G where G is the generation number. The population is expressed as

$$PG = [\overrightarrow{X_{1,G}}, \overrightarrow{X_{2,G}}, \overrightarrow{X_{3,G}}, \dots, \overrightarrow{X_{N,G}}],$$

and $x_{i,G}$ ($i = 1, 2, 3, 4 \dots N$) as 'n' dimensional vector. The population has a sudden variation termed as mutation where a mutant vector is used $\overrightarrow{V_{i,G}}$.

The proposed work follows the mutation strategy of DE/rand/1 and therefore the mutant vector is represented using three random values ($r1, r2, r3$) from its population as in Equation 9.

$$\overrightarrow{V_{i,G}} = \overrightarrow{x_{r1,G}} + F \cdot (\overrightarrow{x_{r2,G}} - \overrightarrow{x_{r3,G}}). \quad (9)$$

Here, F is the amplification factor and its value is considered to be 1. This mutation process paves way to find feasible alternative paths from the mutant node to the destination node. Additionally, the diversity of the mutant vectors is controlled by the crossover mechanism. Few nodes of mutant vector $\overrightarrow{V_{i,G}}$ are interchanged to produce offsprings vector $\overrightarrow{U_{i,j,G}}$ and is given by the Equation 10.

$$\overrightarrow{U_{i,j,G}} = \begin{cases} \overrightarrow{V_{i,j,G}} & \text{if } \text{rand}(0,1) \leq C_r \\ \overrightarrow{x_{i,j,G}} & , \text{ otherwise,} \end{cases} \quad (10)$$

where, $\text{rand}(0,1)$ - Uniformly distributed random values in range (0,1), C_r - Crossover rate where [$C_r = 0.8$].

Finally, the selection phase plays the major role to choose the best fit. Now the generated vector is therefore compared with the other target vector. As the iteration continuous till the termination criterion is met, best secured path will be obtained and the selection factor is as in Equation 11.

$$\overrightarrow{x_{i,G+1}} = \begin{cases} \overrightarrow{U_{i,G}} & \text{if } f(\overrightarrow{U_{i,G}}) \leq f(\overrightarrow{x_{i,G}}) \\ \overrightarrow{x_{i,G}} & , \text{ otherwise.} \end{cases} \quad (11)$$

The algorithm for trusted sensing model using differential evolution is given in Algorithm 1.

Algorithm 1: Trusted Sensing Model using DE

Input: Nodes in MANET, Control parameters in DE

Output: Trusted Secured path for data transmission

-
- Step 1: Population of DE \leftarrow No. of nodes in MANET
 Step 2: Initialize $F=1$, $C_r = 0.8$ and $\Delta T > 0.5$, $NP = 20$
 $F \leftarrow$ Amplification factor //for mutation
 $C_r \leftarrow$ Cross over rate //for crossover
 $\Delta T \leftarrow$ Trust threshold //for path calculation in fitness function
 $NP \leftarrow$ iterations
 Step 3: Initialize all feasible paths / for each solution candidate node. // set $P_G = 0$ and randomly initialize $x_{i,G}$
 Step 4: $i=1$ // iteration count
 Step 5: if path $>$ bestfit_path, STOP
 Step 6: Else
 Step 7: Perform mutation using Equation 9 // explore alternative path
 Step 8: Perform crossover using Equation 10 // explores possible alternative paths and generates trial vector
 Step 9: Selection process using Equation 11 // check trial vector with target vector
 Step 10: $i = NP$ or $i=i+1$ // till termination criteria is met.
 Step 11: END
 Step 12: Secured data transmission through best fit path
 Step 13: If ($Trust_{AB}^{cur} \neq 1$) // presence of packet dropping malicious activity
 Step 14: update trust using Equation 6
 Step 15: Else ($Trust_{AB}^{cur} = 1$) no malicious activity update trust using Equation 7
 Step 16: END
-

4. Parameter Analysis and Result Discussion

The proposed DE based trust model is compared with the other algorithms like GA [1] and routing protocols like DSR [8] and AOMDV [1]. It is analyzed using NS2 simulations and carried out multiple times to obtain the best solution. Table 2 represents the simulation parameters as shown.

Table 2
Simulation Parameters and Mutation Parameters

Parameter	Values
Simulation time	100s
Area Size	1000m ²
Pause time	10s
Traffic type	Constant Bit Rate
Transmission radius	250m
Mobility Model	Random way point
Packet Size	512 bytes
Connection Rate	4 Packets / sec
Amplification Factor (F)	1
Cross Over Rate (Cr)	0.8
Trust Threshold (ΔT)	$\Delta T > 0.5$
No. of iterations (NP)	20

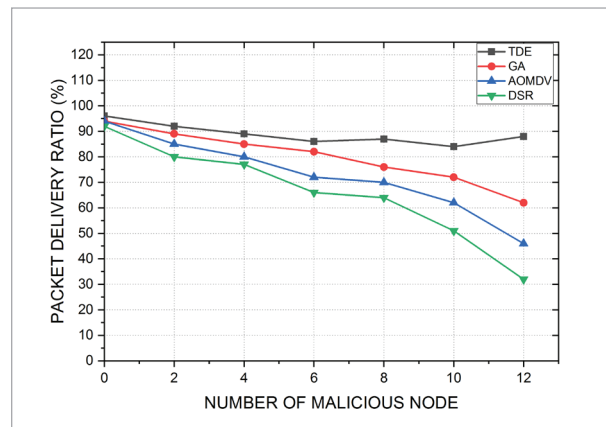
Other parameters such as w_1 , w_2 and ψ are initialized as 0.5, 0.5 and 0.4, respectively. Initially, each node in the MANET is considered with the trust value of 0.5. The simulation has been carried with different node densities as of 50, 100, 150 and 200 nodes. Here, the number of nodes in the network is considered to be the population of the trusted model. The number of malicious nodes tested are 2, 4, 6, 8, 10 upto 20 in multiples of 2 increasing by 2 for 10 different topologies.

4.1. Packet Delivery Ratio (PDR)

The Packet Delivery Ratio represents the total number of successfully delivered data packets to the destination node. Figure 1 shows the packet delivery analysis ratio with respect to the increase in malicious node.

When there is no malicious node, the packet delivery ratio loss is 5% and when there is an increase in the malicious node, the packet delivery loss ratio is drastically increased to 30%. When compared with other techniques, the proposed trusted sensing model degrades gradually as shown in Figure 1. The protocols such as AOMDV and DSR degrades sharply followed by the Genetic Algorithm. The main advantage of the proposed technique is that, the improved distrust factor that induces the algorithm to obtain secured path by inhibiting the malicious node to perform as good ones. When the malicious node increases to 20, there will be a drop of still 15% because of the participa-

Figure 1
Packet Delivery Ratio vs the Number of Malicious Node

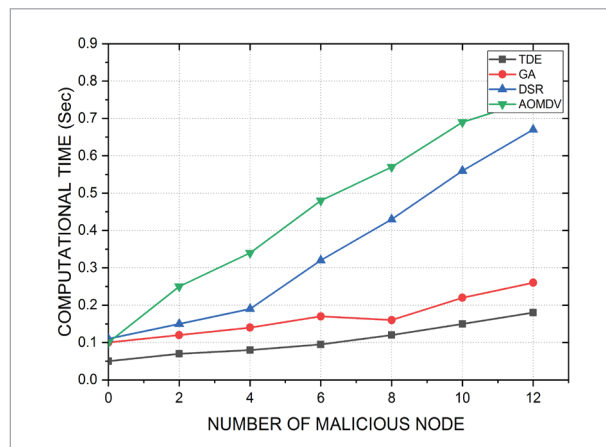


tion of low trusted nodes. Hence, the proposed work achieves 95% to 85% packet delivery ratio, which helps to identify the black hole attack.

4.2. Computation Time

As the proposed work involves Differential Evolution algorithm, it is therefore necessary to compute the computational time to search the efficient route for data transmission. The simulation is carried out for 50 nodes in the MANET under different count of malicious nodes 2, 4, 6, 8 and 10. The simulation stops when it searched the most trusted path to the destination. The chromosomes in the differential evolution algorithm obtain all feasible paths to the destination and finally gets the best suited path (i.e.) best fit chromosome. The overall process is depicted in Figure 2.

Figure 2
Computational time with increased malicious nodes



From the experimental analysis, it is clear that the proposed trusted sensing model using DE requires minimum computational time and does not degrade itself with an increase in malicious nodes. With repeated iterations of the chromosome, exactly suitable routes are obtained. Therefore, the computational time of the proposed is found to be 0.154s and for other algorithms 0.185s for genetic algorithm, 0.421s for DSR and 0.652s for AOMDV.

4.3. Scalability

Considering the scalability factor, the simulation is carried out for 10 different topologies by varying the number of nodes from 20 to 100. For the differential evolution algorithm, the difference vector scheme in the mutation strategy enhances the search method for the best route. The quality of the solution is improved in DE when compared with GA, where maximum trusted node is selected for the path and routing process to transmit data.

References

1. Ahn, C. W., Ramakrishna, R., S. A Genetic Algorithm for Shortest Path Routing Problem and the Sizing of Populations. *IEEE Transactions on Evolutionary Computation*, 2002, 1(1), 511-579.
2. Anjum, A., Mohammed, G. N. Optimal Routing in Ad-Hoc Network Using Genetic Algorithm. *International Journal of Advanced Networking and Applications*, 2012, 03(05), 1323-1328.
3. Chandrasekaran, K, Selvaraj, T. Differential Evolution Capsnet Model for Qos Routing Enhancement in Wireless Networks. *International Journal of Communication Systems*, 2019, e4146. <https://doi.org/10.1002/dac.4146>
4. Chakraborty, U., Das, S., Abbott, U. Clustering in Mobile Ad Hoc Network With Differential Evolution. *IEEE Congress on Evolutionary Computation (CEC)*, 2011, 2223-2228. <https://doi.org/10.1109/CEC.2011.5949890>
5. Govindan, K., Mohapatra, P. Trust Computation and Trust Dynamics in Mobile Ad Hoc Network: A Survey. *IEEE Communication Surveys & Tutorials*, 2012, 14(2). <https://doi.org/10.1109/SURV.2011.042711.00083>
6. Gundry, S., Kusyik, J., Zou, J., Sahin, C. S., Uyar, M. U. Differential Evolution Based Fault Tolerant Topology Control in MANETs. *Military Communications Conference*, 2013. <https://doi.org/10.1109/MILCOM.2013.151>
7. Gundry, S., Zou, J., Kusyik, J., Uyar, M. U., Sahin, C. S. Fault Tolerance Bio-Inspired Topology Control Mechanism for Autonomous Mobile Node Distribution in MANETs. *Military Communications Conference*, 2012. <https://doi.org/10.1109/MILCOM.2012.6415743>
8. Johnson, D., Maltz, D. *Dynamic Source Routing in Ad Hoc Mobile Wireless Networks*. Mobile computing (1st ed.). Kluwer Academic Press, 1996, 153-181. https://doi.org/10.1007/978-0-585-29603-6_5
9. Ren, J., Wang, J., Xu, Y., Cao, L. Applying Differential Evolution Algorithm to Deal With Optimal Path Issues in Wireless Sensor Networks. *IEEE International Conference on Mechatronics and Automation (ICMA)*, 2015, <https://doi.org/10.1109/icma.2015.7237748>. <https://doi.org/10.1109/ICMA.2015.7237748>
10. Storn, R., Price, K. *Differential Evolution - A Simple and Efficient Adaptive Scheme for Global Optimization Over Continuous Spaces*. Technical Report TR-95-012, ICSI, 1995.

5. Conclusion

As the MANET lack central co-ordination, they require full cooperation among the nodes to identify the attacks in the network. The proposed trusted sensing model using the differential evolution algorithm helps to identify the malicious node causing the black hole attack. Here, the data are successfully delivered through a secured communication path which inhibits the malicious node. The key factor, distrust plays a major role in providing secured shortest path and penalty factor reduces the current trust value of the node when it is considered to be malicious. The main benefit of DE is that it inhibits the malicious node to be part of the secured transmission. It has the ability to find the better quality solution, and has better convergence characteristics and efficient computation. Through successive simulations DE have high impact in identification of malicious node rather than other routing protocols DSR, AOMDV and Genetic Algorithm. This work can be further extended to other attacks such as cooperative black hole, gray hole and DDOS attack with different mutation strategy.

11. Subramaniam, S., Saravanam, R., Prakash, P. K. Trust Based Routing to Improve Network Lifetime of Mobile Ad Hoc Networks. *Journal of Computing and Information Technology*, 21(3), 2013, 149-160. <https://doi.org/10.2498/cit.1002139>
12. Sun, Y. L., Yu, W., Han, Z., Liu, K. J. R. Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Network. *IEEE Journal on Selected Areas in Communications*, 2006, 24(2). <https://doi.org/10.1109/JSAC.2005.861389>
13. Wang, B., Gu, L. Detection of Network Intrusion Threat Based on the Probabilistic Neural Network Model. *Information Technology and Control*, 2018, 48(4), 618-625.
14. Wei, W., Qin, Y. and Cai, Z. A Multi-Objective Multicast Routing Optimization Based on Differential Evolution in MANET. *International Journal of Intelligent Computing and Cybernetics*, 2018, 11(1), 121-140, <https://doi.org/10.1108/IJICC-02-2017-0016>
15. Wei, Z., Tang, H., Yu, R. F., Wang, M., Mason, P. Security Enhancements for Mobile Ad Hoc Networks With Trust Management Using Uncertain Reasoning. *IEEE Transaction on Vehicular Technology*, 2014, 63(9). <https://doi.org/10.1109/TVT.2014.2313865>
16. Xia, H., Jia, Z., Li, X., Ju, L., Sha, E. H.-M. Trust Prediction and Trust-Based Source Routing in Mobile Ad Hoc Network. *Ad Hoc Network*, 2013, 11, 2096-2114. <https://doi.org/10.1016/j.adhoc.2012.02.009>
17. Xia, H., Wang, G.-D., Pan, Z.-K. Node Trust Prediction Framework in Mobile Ad Hoc Network. *IEEE: Trustcom/BigDataSE/ISPA*, 2016, 50-56. <https://doi.org/10.1109/TrustCom.2016.0045>
18. Yetgin, H., Cheung, K. T. K., Hanzo, L. Multi-Objective Routing Optimization Using Evolutionary Algorithms. *IEEE Wireless Communication and Networking Conference (WCNC)*. <https://doi.org/10.1109/WCNC.2012.6214324>

