Turkish Journal of Computer and Mathematics Education *Vol.12 No.3(2021), 4349-4356*

Research Article

Strong Secure Anonymous Location Based Routing (S2ALBR) method for MANET

Mrs. Swetha M S[a], Dr. Pushpa S K[b] , Dr.Thungamani M[c] , Dr. Manjunath T N[d], Dr. Deepak S Sakkari [e]

[a]Research Scholar, Dept. of ISE, BMS Institute of Technology and Management, Bengaluru, India
[b]Assistant Professor, Dept. of CSE, GKVK, UOH, Bengaluru, India
[c]4 Professor, Dept. of ISE, BMS Institute of Technology and Management, Bengaluru, India
[d]Assistant Professor, Dept. of CSE, Presidency University Bengaluru, India

[a]swethams_ise2014@bmsit.in, [b]pushpask@bmsit.in , [c]thungamani_k@rediffmail.com , [d]manju.tn@bmsit.in, [e]deepakssakkari@presidencyuniversity.in

Article History: Received: 10 November 2020; Revised 12 January 2021 Accepted: 27 January 2021; Published online: 5 April 2021

Abstract: Mobile Ad Hoc Networks (MANETs) utilize confounding planning shows that spread community point characters similarly as courses from outside onlookers so as to give obscurity security. MANET contains different little gadgets conceding suddenly over the air. The topology of the system is changing an incredible piece of the time in light of the advantageous idea of its inside focuses. The security challenges ascend taking into account self-game-plan and self-reinforce limits. By the by, existing mysterious organizing shows depending upon either ricochet by-skip encryption or excess traffic either produce imperative expense or can't give full namelessness security to information sources, targets, and courses. The imperative expense raises the trademark asset limitation issue in MANETs particularly in natural media remote applications. To offer high absence of definition assurance expecting for all intents and purposes no effort, we strong secure anonymous location based routing (S2ALBR) protocol for MANET utilizing optimal partitioning and trust inference model. In S2ALBR appear, first segments a system into zones utilizing optimal tug of war partition (OTW) algorithm. By at that point, figure the trustiness of each reduced focus point utilizing the imprisonments got signal quality, versatility, way debacle and joint exertion rate. The arrangement of trust calculation is advanced by the optimal decided trust inference (ODTI) model, which gives the trustiness of each adaptable. By then picks the most basic trust ensured focus point in each zone as generally engaging trade habitats for information transmission, which structure a non-unquestionable bewildering course. The introduction of proposed S2ALBR show is examined by various testing conditions with Network Simulator (NS2) instrument.

Keywords: Strong secure anonymous location based routing (S2ALBR) Optimal tug of war partition (OTW), optimal decided trust inference (ODTI).

1. Introduction

MANET includes focuses that can converse with one another through remote mediums. [can use - focuses/mode/technique]These focuses fill in as an end structure, yet in like manner as a change to impel packs to other people, without the guide of any present foundation or united affiliation [1]. It is hard to give trusted and guarantee about correspondences in inadequately organized conditions, for example, front lines. Organizing controlling shows for such a not all around masterminded conditions is an affecting errand in MANET[networks]due to getting away from hand of focuses [2].The essential for flaw tolerant and guarantee about planning shows was seen to address planning in gravely orchestrated conditions, unequivocally inside observing harmed focuses, by investigating system redundancies [3,4].

Secrecy in MANETs joins character and area riddle of information sources (i.e., senders) and goals (i.e., beneficiaries), comparably as course dimness. "Character and domain puzzle of sources and targets" hints it is hard if achievable for different focus focuses to pick up the genuine characters and mindful areas of the sources and goals. Moreover, so as to confine the relationship among source and target (i.e., relationship nuance [11]), it is fundamental to shape a dark course between the two endpoints and affirmation that middle focuses in movement don't have the foggiest idea where the endpoints are, particularly in MANETs where area gadgets might be prepared. Existing absence of definition planning appears in MANETs can be fundamentally depicted into two classes: jump by-ricochet encryption [12], [13], [14], [15], [16] and excess traffic [17], [18], [19], [20]. A gigantic portion of the present strategies are limited by concentrating on keeping up riddle at a stunning expense to significant assets since open key-based encryption and high traffic produce fundamentally critical expense. Likewise, different ways of thinking can't give the total of the as of late referenced namelessness affirmations.

2. Literature Survey

Zhang et al. [11] have presented a bio-awakened mutt confided in coordinating show (B-iHTRP) considering trusted in examination, physarum autonomic optimization (PAO) and ant colony optimization (ACO). Firstly, they brought the cross-layer perception into ACO to secure perceiving ants. Inside each zone, the course table was kept up proactively by the sharp ants which can distinguish concerned parameters. Among zones, the observing ants are sent to responsively find courses to objectives while identifying concerned parameters. Additionally, B-iHTRP uses PAO to pick the perfect one from the found courses and autonomic development the local courses over the range of multi-zone correspondence gatherings. The mix of ACO and PAO procedure improve the show effectively, anyway more awful than DHT based controlling because of high essentialness usage.

Biswas et al. [12] have proposed a response for recognizing and avoiding dim opening ambushes and ensuring secure pack transmission close by powerful resource utilization of versatile has all the while. According to their recommendation, appraisal of trust of every center in the framework relied upon parameters, for instance, steadfastness of a center portrayed by its transportability and relief time, remaining battery power, etc. The trust of a center point shapes the reason of assurance of the most strong course for transmission. In spite of the way that the procedure gives extraordinary execution to the extent throughput, secure directing, and powerful resource use, anyway doesn't improve the display unfathomably.

Abid et al. [13] have proposed a DHT-based coordinating show which abuses a 3D canny space that considers the physical intra-neighbor associations of a center point and tries a 3D structure to unravel that relationship. Each center point runs a passed on count to procure a consecutive rational identifier that reflects its physical closeness in the 3D real space. Also, the show utilizes the 3D-structure to keep up multi-approaches to an objective center point in order to address the adaptability issue and increment adaptability against a center point/interface dissatisfaction. The methodology beats than other DHT-based coordinating show in wording guiding overhead, through and through deferral, way stretch characteristics and pack movement extent. It isn't fitting for high thickness mastermind because sort out lifetime is low.

Uddin et al. [14] have proposed uncommonly selected on demand multipath detachment vector show with the Fitness Function (FF-AOMDV). The health work was used to find the perfect path from the source to the objective to lessen the imperativeness use in multipath coordinating. FF-AOMDV strategy beat than AOMDV and AOMR-LM under bigger piece of the framework execution estimations and parameters. In light of the malignant ambushes the data transmission is impacted with inside module.

Ejmaa et al. [15] have proposed a neighbor-based dynamic connectivity factor routing protocol (DCFP), which had the choice to logically test the status of the key structure without the intercession of a system chief subject to a novel structure metric, while decreasing the RREQ overhead using another accessibility factor. The DCFP beats than both NCPR and AODV to the degree from beginning to end delay, sorted out organizing overhead, MAC impact, centrality use, mastermind system and pack advancement degree.

Smith et al. [16] have developed a SUPERMAN structure for secure correspondence. The structure was required to allow existing framework and controlling shows to play out their abilities, while giving center confirmation, find a better than average pace, correspondence security areas. The fundamental spot was to secure access virtually closed network (VCN) that licenses beneficial, trustworthy correspondence with confirmation, steadfastness and validity affiliations. SUPERMAN gives lower-cost security than others for their differing arranging shows up. In any case, impact rates are not created stood separated from DCFP.

Shen et al. [17] have proposed anonymous location-based and efficient routing protocol (ALERT). ALERT capably parcels framework field into zones and capriciously takes centers in zones as commonly captivating hand-out center centers, which structure a non-perceivable cloud course. Specifically, in each arranging improvement, a data sender or forwarder zones the framework field in order to isolate itself and the objective into two zones. It by then discretionarily picks an inside point in the other zone as the going with hand-to one side and send the data to the hand-to one side. In the last headway, the data is given to k center concentrations in the objective zone, giving k-nonappearance of clearness to the objective. ALERT has a system to cover the data initiator among different initiators to stimulate the riddle security of the source. ALERT is in like manner versatile to intersection point and timing ambushes.

Defrawy et al. [18] have proposed an anonymous location-aided routing in MANETS (ALARM), which demonstrated that feasibility of at the same time getting, strong insistence, and security properties, with reasonable reasonableness. The standard seeing component of the envisioned area based MANET condition is the correspondence perspective, set up not concerning perpetual or semi-constant characters, domains or pseudonyms, transient center point zone. At this moment, proposes center point nonappearance of clearness and security from following. In spite of the way that it might give the likelihood that our security and affirmation properties disrespect each other.

3. Proposed System

S^2ALBR protocol is represented in Fig. 1, it comprises of cluster head nodes (CHs) and mobile nodes (cluster member) and Malicious node (MN). Cluster head node utilized to gather the information from the mobile nodes. Primarily, mobile nodes are arbitrarily distributed in the network. Subsequent to formation of cluster, we have to calculate the trust degree of each node utilizing some groups of metrics. Due to continuous data transfer in same node, high energy loss will be occurred. The greatest trust degree node is work as CH among multiple nodes in the cluster. CH is accountable to collect data information from cluster components and more promote to Destination in the network.Compare to existing protocol, we have maximized the network lifetime, throughput and minimize the delay, energy consumption, number of dead nodes, loss ratio.

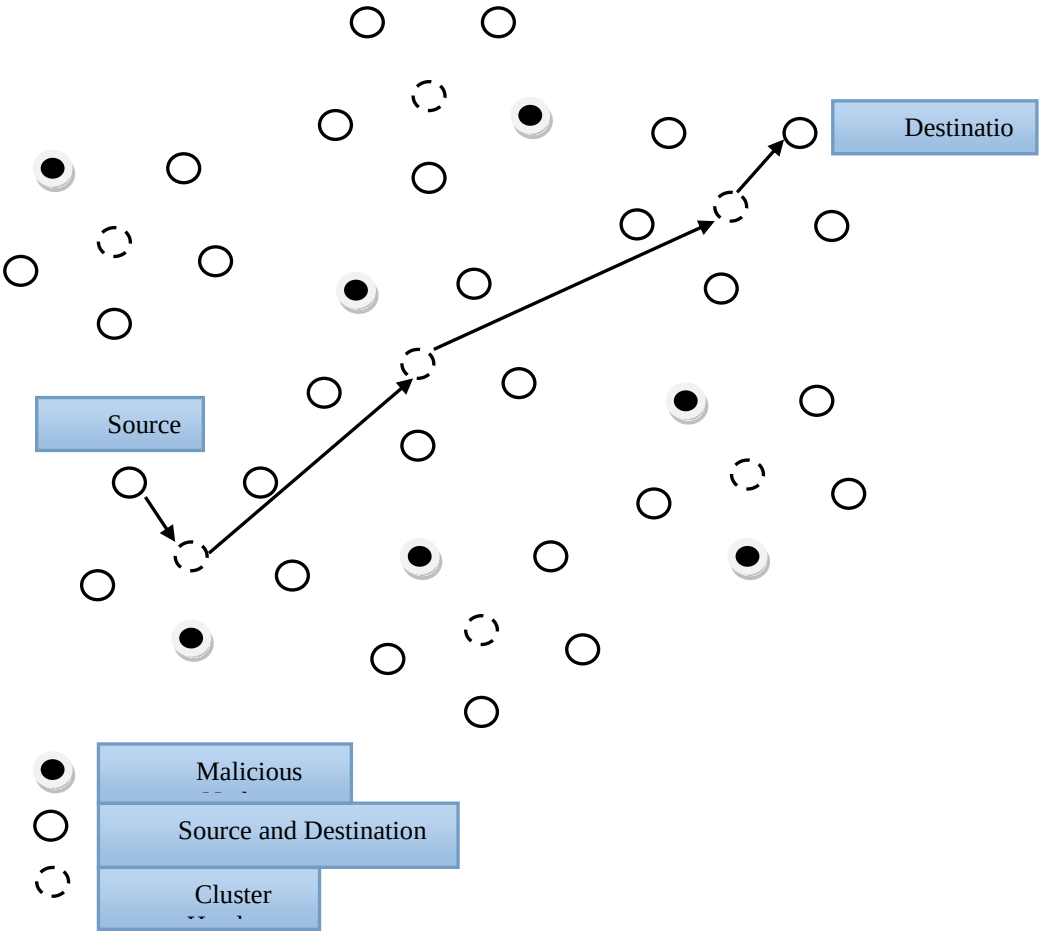

Fig.1 Network model of proposed S^2ALBR protocol

4. Proposed S2ALBR protocol using OTW and ODTI technique

4.1. Cluster formation using (OTW) algorithm

A myopic version of the global energy-system model used to reduce foresight causes postponement of investments in new technologies leading to higher investment needs in the future and a higher reliance on fossil fuels in the near term. Myopic models can be a valuable complement for perfect foresight (PF) optimization models. Where PF models used to identify optimal transition pathways, myopic model versions could serve to provide more realistic projections of likely scenarios for the evolution of the electricity system. Moreover, using both approaches in parallel could facilitate assessing both the effectiveness and efficiency of certain policy instruments. An important advantage is that the ideal and likely scenarios can be generated within a single framework as using a myopic model version requires only minor changes to the model. Another welcome advantage of myopic model versions is that the shorter time horizon reduces the computational cost. A natural heuristic policy one may consider for a stochastic depletion problem is given by the myopic policy which in state S chooses an activity set S_A that maximizes expected reward earned over the following time-step.

$$\prod^{g}(S) \in \arg\max_{a \in S_A} E[R(S, S_A)] \tag{1}$$

Such a policy is adaptive but ignores the evolution of the system and the impact of the present choice of activity on rewards in future states. The set S_A in myopic problem above is potentially exponentially large. Set is an implicit polynomial sized representation and myopic maximization problem is efficiently solved. Myopic maximization problem is difficult but one has access to an appropriate near-optimal oracle.Here, we utilize the improved myopic algorithm for CH selection process with multiple constraints such as energy consumption, network lifetime, routing cost, network load and distance. An improved myopic heuristic reward incurred in choosing activity S_A at some state s is independent of the past. The expected total reward earned under the myopic heuristic in this clairvoyant scenario is equal to the expected total reward earned under the myopic heuristic for the corresponding sample path. We will compare the performance of the improved myopic heuristic to that of an optimal clairvoyant algorithm that knows the realizations of the Pt processes a-priori. Since an optimal clairvoyant policy must dominate the optimal policy, it will suffice to demonstrate performance guarantees relative to the optimal clairvoyant policy. Thus,

$$S_A = \left(\min\left(E_T, RC, L_{nw}, D\right) \cup \max\left(T_{nw}\right) : 0 < t \le T\right) \tag{2}$$

In the sequel, we will only consider such optimal policies; any reference to an optimal policy or value function in the sequel will pertain to an optimal policy or value function for the clairvoyant problem. Now, the best optimal value owned sensor node in the cluster set is elected as CH node.

$$CH_i = \sum_{i=1}^{n} S_{A_i} \tag{3}$$

Finally, the Brown function [34] used to crosscheck the elected CH node as follows:

$$F(S_A) = \sum_{i=1}^{n} \left(S_{A_i}^2\right)^{\left(S_{A_{i+1}}^2 + 1\right)} + \left(S_{A_{i+1}}^2\right)^{\left(S_{A_i}^2 + 1\right)} \tag{4}$$

Especially, when a large number of sensor nodes are deployed in an area, a node has several adjacent neighbors equipped with the same sensing equipment, so that the network will be able to cope with the failure of some nodes. Thus, the time until the first node died is not the only metric to evaluate the network lifetime. As a result, the lifetime that a part of nodes die is a more effective metric when evaluating the performance in scenarios of high node density. Since network connectivity is affected by the node density, a lifetime definition based on the percentage of dead nodes can reflect other lifetime definitions based on connectivity and/or coverage. The lifetime of sensor i , t_i depends on the maximum number of packets that can be transmitted by the sensor to the sink. Since the time duration for transmitting a packet is very short, it can be neglected in the analysis of the sensor lifetime.

$$t_i = \sum_{j=1}^{[p_i]} \lambda^{p_1} \frac{x^{p_1 - 1} e^{-\lambda\tau}}{\Gamma(p_i)} \tag{5}$$

where p_i represents the maximum number of packets that sensor i can transmit during time τ Then, lifetime of the network as follows:

$$NLT = T\left[\max\left(t_i\right) \in \frac{N_a}{N}\right] \tag{6}$$

where N is the number of sensors in the network and N_a is the number of alive nodes. The route cost (RC) between two nodes are defined as follows,

$$RC(n, d) = \sum_{i, j \in (n, \cup, d)} \text{cost}_{i,j} \tag{7}$$

where $\text{cost}_{i,j}$ cost function for a link between nodes i and j. Thus,

$$\text{cost}_{i,j} = E_p + 2\,N\,E_{tx}(n,d) + e^{\frac{1}{E_R^i}} \tag{8}$$

where E_R^i is cost function that takes into consideration the remaining energy of sensors for the energy balance among sensors.

The acceleration of an agent is computed by taking total forces from a group of heavier masses and it is based on the law of gravity equation (6) and it is calculated based on the law of motion (7). The velocity of an agent is calculated by taking the fraction of its current velocity adding to its acceleration (8) and next position is calculated by the equation (9).Afterwards, next velocity of an agent is calculated as a fraction of its current velocity added to its acceleration (Eq. (9)). Then, its next position can be calculated using Eq. (10):

$$F_i^d(t) = \sum_{j \in kbest,\, j \neq i} rand_j G(t) \frac{M_j(t) M_i(t)}{R_{ij} + \varepsilon} \left(x_j^d(t) - x_i^d(t) \right) \tag{9}$$

$$a_i^t(t) = \frac{F_i^d(t)}{M_i(t)} = \sum_{j \in kbest,\, j \neq i} rand_j G(t) \frac{M_j(t)}{R_{ij} + \varepsilon} \left(x_j^d(t) - x_i^d(t) \right) \tag{10}$$

$$V_i^d(t+1) = rand_i \times V_i^d(t) + a_i^d(t) \tag{11}$$

$$X_i^d(t+1) = X_i^d(t) + V_i^d(t+1) \tag{12}$$

where $rand_i$ and $rand_j$ indicates uniformly distributed random number present in the interval [0,1], ε indicate the small value, $R_{ij}(t)$ indicate the Euclidean distance between two agents i and j and it is defined as $\|X_i(t)X_j(t)\|_2$. The set of first K agents is given as Kbest which include best fitness value and biggest mass. The K indicate the function of time and the initial value is given by $K_{initial}$ value and value will decrease with time. G(t) indicate the gravitational constant and the initial value is given by $G_{initial}$:

$$G(t) = G(G_{initial}, G_{end}, t) \tag{13}$$

To balance its intensification and diversification in gravitational search algorithm (GSA) the two main components used are the K and G. In order to avoid trapping in the local optimum diversification is used at initial iterations. Addition of high values to K and G parameters in the initial stage is considered as important step in the GSA and it is indicated as $K_{initial}$ and $G_{initial}$. If high vaue K is used then the mass will be moved to the search space based on the position of more masses and this will increase the diversification of algorithm. If the high value G is used it will increase the mobility of each mass present in the search space and here also the diversification of algorithm is increases. Therefore it is assumed that by using high value K and G parameters best solution space can be identified.

For different iterations the diversification of GSA must fade out and the intensification of it must fade in. By reducing the K and G in the laps, this can be achieved. The low value of K parameter will move the mass to the search space based on the position of few masses and the intensification of algorithm increases. The mobility mass present in the search space will decrease with low G value. This will increase intensification of the algorithm. For finding the location of the application nodes (AN) are calculated here. Consider the initial energy as $E_j(0)$, the data transmission rate is given by r_j, the distance –independent parameter is given by a_{j1} and the distance-dependent parameter of the j^{th} AN is given by a_{j2}. The lifetime ($l_{ij}(t)$) is given by:

$$l_{ij}(t)=\frac{E_j(0)}{r_j(a_{j1}+a_{j2}\,d_{ij}^{n})} \tag{14}$$

Where d_{ij}^{n} indicate n-order Euclidian distance. The fitness function is given by:

$$f_i(t)=\underset{j\in\{1,\ldots\ldots m\}}{Min}\, l_{ij}(t) \tag{15}$$

Where number of AN is given by m. If the fitness value is high then the lifetime is high.

4.2 Cluster trust value computation using ODTI model

The optimal decided trust inference (ODTI) model, streamlining routine is a developmental procedure that is reasonable to take care of an assortment of advancement issues that lie outside the extent of the standard enhancement strategies. For the most part, cluster has the upside of being extremely straightforward in idea, simple to actualize and computationally proficient. In contrast to other heuristic calculations, for example, hereditary calculations, PS has an adaptable and well-adjusted administrator to upgrade and adjust the worldwide and calibrate neighborhood search. A valuable audit of direct scan strategies for unconstrained advancement, though subtleties of the execution embraced in this paper. These returns by figuring a succession of focuses that may not move toward the ideal worth. The calculation begins by building up a lot of focuses called a work, around the given point. This present point could be the underlying beginning stage provided by the client or it could be registered from the past advance of the calculation. The work is shaped by adding the present point to a scalar several of a lot of vectors called an example. In the event that a point in the work is found to improve the target work at the present point, the new point turns into the present point at the following cycle.

5. Results and Discussion

The proposed strong secure anonymous location based routing (S^2ALBR) protocol technique is employed on 50, 100, 150, 200 and 250 node network to illustrate its effectiveness, which used tomaximize theenergy efficient in sensor nodes usingoptimal tug of war partition algorithm and optimal decided trust inference model. The optimal tug of war partition approach used to select the trusted node and shortest node for data transmission from source to cluster head. Our proposed model was compared with ALERT [17], ALARM [18] and AASR [19], and our proposed protocol provide better results by minimizing the parameters delay, energy consumption, latency, routing overhead, lossratio; and maximize the throughput, network lifetime, delivery ratio. The proposed technique is tested using NS-2 simulator and the obtained results are given below in three type of scenario.

5.1 Varying Number of Attacks

In this test, we vary the number of attacks as 50, 100, 150, 200 and 250 given in Table 1. The performance evaluation and the result comparison of proposed S^2ALBR protocol and existing ALERT [17], ALARM [18] and AASR [19] protocol is given table 1

The simulation result of proposed and existing algorithms with 4 performance metrics namely: Energy, Delay, Network Lifetime and Throughput. The nodes are set from 50 to 250 randomly. The energy consumption of proposed and previous routing protocol is given in It is shows the lighting up for containment in centrality use in the structure with high thickness focus fixations as 50 to 250 concerning the particular existing building conventions respectively. Our proposed algorithm reduced a delay when compare to previous one. From 50 to 250 nodes the delay was minimized 20% to 11%. By using 50 to 250 nodes, we are going to maximize the network lifetime with our proposed model and compared with previous method. The performance evaluation of our model generate from 5% to 9%. We maximized the throughput with our proposed method, when compared to previous protocol. The performance evaluation of 50 to 250 nodes again from 5%to 9% and results is shown From the result, it has proved the performance of routing protocol decreases when the malicious node exists in the network. The routing protocol performance increases only when the number packets delivered without malicious node.

Table: 1 Comparison existing protocol with proposed S2ALBR with 4 different metrics by varying number of attacks

Number of attacks	Delay				Energy consumption				Network lifetime				Throughput			
	S2ALBR	ALERT	ALARAM	AASR	S2ALBR	ALERT	ALARAM	AASR	S2ALBR	ALERT	ALARAM	AASR	S2ALBR	ALERT	ALARAM	AASR
50	1	2	2	1	1	2	2	4	5	0	1	0	7	2	2	1
100	3	3.10	3.50	2	2	4	3	5	6	4	2	1	7.10	3	3.50	2
150	5	3.15	3.9	3.30	3	7	5.20	6.20	7	5.50	3.10	3.10	7.30	3.10	3.90	3.10
200	7.10	4.10	4.20	4.30	4.10	9.20	6.10	8.50	8.10	6.70	6	4.10	8.10	4.20	4.20	4.50
250	11.20	5.8	4.50	5.10	6.50	11.10	9.10	9.10	9.50	7.10	6.10	5.10	9.10	5.60	4.50	5.20

5.2 Varying Number of Nodes

In this test, varying the number of mobiles node from 50, 100, 150, 200 and 250 in the fixed network area. The performance comparison of proposed S^2ALBR and existing ALERT [17], ALARM [18] and AASR [19] protocol is given in table 2.

By varying number of nodes from 50 to 250 randomly the performance metrics of proposed and previous routing protocol is given in the delay were minimized from 29% to 5% respectively and shown in Then energy was increased from 8% to 10%. The network lifetime and throughput also increased and the values are shown in below table

Table: 2 Comparison existing protocol with proposed S2ALBR with 4 different metrics by varying number of nodes

Number of nodes	Delay				Energy consumption				Network lifetime				Throughput			
	S2ALBR	ALERT	ALARAM	AASR	S2ALBR	ALERT	ALARAM	AASR	S2ALBR	ALERT	ALARAM	AASR	S2ALBR	ALERT	ALARAM	AASR
50	77	42	32	35	1	3.10	5.50	4.50	51.10	1	13	12	74	42	37	35
100	78	43	43	42	2	5.80	6.10	5.00	63.20	32	32	22	78	54	47	42
150	79	55	55	52	3	6.10	7.90	6.10	64.30	59	44	35	79	64	55	52
200	80	67	69	70	4.10	7.60	8.10	7.10	73	64	46	36	76	67	67	70
250	83	74	79	73	5.50	8.50	9.10	8.10	80.10	77	59	38	84	70	79	73

6. Conclusion

In this paper, we have proposed a strong secure anonymous location based routing (S^2ALBR) protocol for MANET. The proposed S^2ALBR protocol consists of two processes are clustering and path selection. The proposed optimal tug of war partition algorithm is utilized to form the clustering and the multiple performance constraints used to compute the trust degree of each node. The highest trust degree is act as CH in the cluster among multiple mobile nodes. The optimal decided trust inference model is used to compute the optimal path among multiple paths. Finally, the proposed S^2ALBR protocol is applied to ODTI model to evaluate the performance. The simulation results proved that the effectiveness of proposed S^2ALBR protocol in terms of throughput, delay, energy and network lifetime.

References

HoudaMoudni , Mohamed Er-rouidi," Secure Routing Protocols for Mobile Ad Hoc Networks", Information Technology for Organizations Development (IT4OD), 2016

B. John Oommen , SudipMisra," Fault-tolerant routing in adversarial mobile ad hoc networks: an efficient route estimation scheme for non-stationary environments",Telecommunication Systems, Volume 44, Issue 1–2, pp 159–169, 2010

B. John Oommen ,SudipMisra," Fault-tolerant routing in adversarial mobile ad hoc networks: an efficient route estimation scheme for non-stationary environments"Telecommunication Systems, Volume 44, Issue 1–2, pp 159–169, 2010

Yuan Xue , Klaranahrstedt," Providing Fault-Tolerant Ad hoc Routing Servicein Adversarial Environments,Wireless Personal Communications, Volume 29, Issue 3–4, pp 367–388, 2004

KimayaSanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, Elizabeth M. Belding-Royer. "A Secure Routing Protocol for Ad Hoc Networks," In Proc. of IEEE International Conference on Network Protocols (ICNP). 2002

E. Royer and Chai-KeongToh. A review of current routing protocols forad hoc mobile wireless networks. Personal Communications, IEEE, 1999.

Sheng Liu, Yang Yang, Weixing Wang," Research of AODV Routing Protocol for Ad Hoc Networks",AASRIProcedia,Volume 5, Pages 21-31,2013

S. Mohapatra, P.Kanungo," Performance analysis of AODV, DSR, OLSR and DSDV Routing Protocols using NS2 Simulator",Procedia Engineering, Volume 30, 2012, Pages 69-76

SalwaOthmen , FaouziZarai, AymenBelghith, LotfiKamoun," Anonymous and Secure On-Demand Routing Protocol for Multihop Cellular Networks", Networks, Computers and Communications (ISNCC), 2016

Uma Rathore Bhatt ,NeeleshNema, RakshaUpadhyay," Enhanced DSR: An Efficient Routing Protocol for MANET", Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014

Mingchuan Zhang, Meiyi Yang, Qingtao Wu, RuijuanZheng, and Junlong Zhu," Smart Perception and Autonomic Optimization:A Novel Bio-inspired Hybrid Routing Protocol for MANETs"Future Generation Computer Systems ,Volume 81, Pages 505-513, 2018

SuparnaBiswas, Tanumoy Nag, SarmisthaNeogy," Trust Based Energy Efficient Detection and Avoidance of Black Hole Attack to Ensure Secure Routing in MANET" Applications and Innovations in Mobile Computing (AIMoC), 2014

S.A. Abid, Mazliza Othman, Nadir Shah, Mazhar Ali , A.R. Khan," 3D-RP: A DHT-Based Routing Protocol for MANETs" The Computer Journal , Volume: 58, Issue: 2, 2015

MueenUddin, AqeelTaha, RaedAlsaqour , TanzilaSaba," Energy Efficient Multipath Routing Protocol for Mobile ad-hoc Network Using the Fitness Function", IEEE Access ,Volume: 5,2017

Ali Mohamed E. Ejmaa , ShamalaSubramaniam, Zuriati Ahmad Zukarnain, ZurinaMohdHanapi," Neighbor-based Dynamic Connectivity Factor Routing Protocol for Mobile Ad Hoc Network" IEEE Access , Volume: 4,2016

Darren Hurley-Smith, Jodie Wetherall , Andrew Adekunle," SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks" IEEE Transactions on Mobile Computing , Volume: 16, Issue: 10, 2017

H. Shen and L. Zhao, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs", IEEE Transactions on Mobile Computing, vol. 12, no. 6, pp. 1079-1093, 2013.

K. El Defrawy and G. Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs", IEEE Transactions on Mobile Computing, vol. 10, no. 9, pp. 1345-1358, 2011.

W. Liu and M. Yu, "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments", IEEE Transactions on Vehicular Technology, vol. 63, no. 9, pp. 4585-4593, 2014.

A. Pfitzmann, M. Hansen, T. Dresden, and U. Kiel, "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management a Consolidated Proposal for Terminology, Version 0.31," technical report, 2005.

Sk.Md.M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, "An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks," Proc. Int'l Symp. Applications on Internet (SAINT), 2006.

Z. Zhi and Y.K. Choong, "Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy," Proc. Third Int'l Workshop Mobile Distributed Computing (ICDCSW), 2005.

V. Pathak, D. Yao, and L. Iftode, "Securing Location Aware Services over VANET Using Geographical Secure Path Routing," Proc. IEEE Int'l Conf. Vehicular Electronics and safety (ICVES), 2008.

K.E. Defrawy and G. Tsudik, "ALARM: Anonymous LocationAided Routing in Suspicious MANETs," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2007.

K.E. Defrawy and G. Tsudik, "PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs)," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2008.