INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2021, VOL. 67, NO. 3, PP. 425-430
Manuscript received May 7, 2021; revised July, 2021 DOI: 10.24425/ijet.2021.137829

An Authenticated Routing Protocol for Wireless Ad Hoc Network Based on Small World Model

Daxing Wang, and Leying Xu

***Abstract*—Compared with traditional cellular networks, wireless ad hoc networks do not have trusted entities such as routers, since every node in the network is expected to participate in the routing function. Therefore, routing protocols need to be specifically designed for wireless ad hoc networks. In this work, we propose an authenticated routing protocol based on small world model (ARSW). With the idea originating from the small world theory, the operation of the protocol we proposed is simple and flexible. Our simulation results show the proposed ARSW not only increases packet delivery ratio, but also reduces packet delivery delay. In particularly, Using authentication theory, the proposed ARSW improves communication security.**

***Keywords*—small world model, wireless Ad Hoc network, routing protocol, AODV protocol, authentication theory**

I. Introduction

IN any network, whether wired or wireless, routing is an important function. Ad Hoc is a wireless self-organizing mobile communication network [1], and its network topology changes frequently in a short time. Therefore, long-term stable routing protocols based on network topology cannot be applied due to the long convergence time of the algorithm. In addition, Ad Hoc network wireless transmission is based on receiving and sending information when sharing bandwidth on the same frequency. The limitation of channel bandwidth and the large business requirements, as well as the increase in routing management transmission overhead due to widespread node movement, these contradictions are very prominent [2]. Existing Ad Hoc network routing protocols still face some problems, for example, the management and control overhead required for routing table creation and maintenance is huge, and the protocol efficiency is very low [3-6].

AODV (Ad Hoc On-demand Distance Vector) is a reactive routing protocol developed for Ad Hoc networks [7-8]. In AODV, whenever a node needs to send data to another node, and when it has no route to that node, it tries to find a new route [9]. Route discovery is accomplished using a route request (RREQ) message. Thus, a node that needs to discover a route to another node sends out a RREQ message. The RREQ contains the IP address of the node originating the request and the IP address of the destination node, that is, the node the originator is trying to reach [10]. In 2004, Kargl F., Schlott S. & Weber M. proposed Secure AODV (SAODV) to protect routing messages exchanged in AODV [11]. SAODV provides some security features, such as routing data integrity, authentication, and non-repudiation [12].

Small world network has the characteristics of small world, that is, high clustering coefficient and short average path length. The establishment of a small world network model has been actively discussed [13]. For example, By randomly adding or switching links, the Newman-Watts (NW) and Watts-Strogatz (WS) models construct a small world network from regular ring lattice. The small world network model can shorten the average path length while maintaining connectivity, which is just suitable for ad hoc networks [14, 15].

Through the further study of the degree distribution of nodes in the world wide web, it is found that the random network represented by the random model cannot correctly explain the existence of distributed nodes in the real network [16]. Guidoni, D. L., mini, R. A. F., & Loureiro, A. A. F. propose an algorithm based on the characteristics of small world, which limits the number of intermediate nodes in the process of message propagation, but does not consider the energy consumption and social authority of nodes [17]. Zhang, J. & Elkashlan M. proposed a small world network construction method of energy saving, which added quick links to ad hoc network with a certain probability, reducing data acquisition delay [18]. However, there are hub nodes in the small world network topology. Therefore, the network lifetime is limited. Small-world phenomena are common in a large number of real networks, such as the computer Internet, scientists' cooperation network, product generation network, and national power network. Zarepour, M. studied the game process of different network structures such as regular network, small world network and random network [19]. Recently, related studies have shown that some heterogeneous wireless networks, such as wireless Ad Hoc networks, also exhibit small-world properties [20].The purpose of this paper is to point out that the relationship between the nodes of the wireless Ad Hoc network has small world characteristics, and to propose an authentication routing protocol based on the small world model for Ad Hoc network. The remainder of this paper has three sections. The first section corresponds to the description of the small model. The second section proposes the new small world model and an authenticated routing protocol based on small world model (ARSW). At last, the three section presents the performance analysis and conclusion of this research.

This work was supported by the key projects of natural science research of the higher education institutions of Anhui (project number: KJ2020A0712), Chu-zhou university scientific research startup Fund Project (project number: 2020qd41) Anhui economic statistics teaching team (project number: 2 019jxtd110).

Daxing Wang is with college of mathematics and finance, Chuzhou Univers ity (e-mail: daxingwang@chzu.edu.cn).

Leying Xu i s with college o f mathematics and finance, Chuzhou University (e-mail: starleewipm@126.com).

II. SMALL WORLD NETWORK MODEL

In the small world model, each node shows certain interests that can be captured, and the content saved by the nodes with similar interests and the submitted queries also show a certain correlation, and the nodes are related according to their performances. Form a network so that nodes with high correlation are relatively close in the network. This kind of network formed by the correlation between nodes shows the characteristics similar to social network, which is called "Small World". Small world phenomenon, that is, the theory that most people are connected by many short chains made of acquaintances, it is caused by Stanley Milgram was first proposed as a sociological issue in the 1960s. There is currently no precise definition of "small world phenomenon". A reasonable explanation is that the average distance L of any two points in the network increases logarithmically with the size of the network (the number of nodes N), that is, L ~ lnN, that is When the number of nodes increases rapidly, the change of L is relatively slow. This phenomenon is called "small world phenomenon". In the Stanley Milgram experiment, the average distance of letter transmission is 6, that is, 6 people can connect two people. American physicists analyze the data collected on the Internet through software. The results show that the characteristic path length in the Internet can reach up to 19 links. From the perspective of Internet routing links, the number of Internet routers is very large, but the average distance between two routers is about 10.

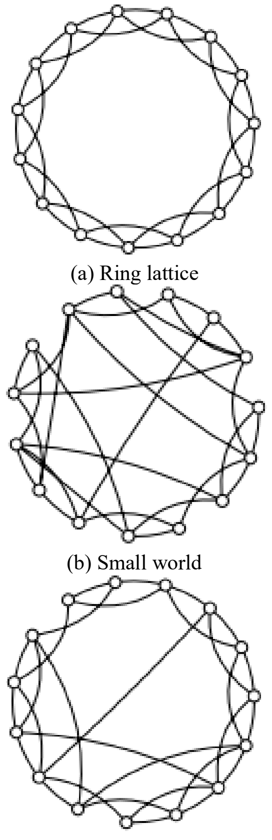
Each point in the small-world network diagram represents a node in the network. If there is a connection between the two nodes, it means that there is a relationship between the two elements represented by the node. The small world network is a network between a structured network and a random network, as shown in Figure 1. In such a network, if a node wants to connect with its non-adjacent nodes, it needs to pass through multiple interrelated intermediate nodes [21]. The relationship between nodes in a random network is completely random and has no regularity. In this network model, the small-world network graph is obtained by adding certain randomness to a structural graph, such as 1-lattice graph. A d-lattice graph is a structure graph obtained according to certain rules. If each node y in the graph is to be added to its associated nodes x_i and z_i, the rules are as follows:

$$x_i = [(y - i^{d'}) + n] \bmod n \tag{1}$$

$$z_i = [(y - i^{d'}) + n] \bmod n \tag{2}$$

Where $1 \leqslant i \leqslant k/2$; $1 \leqslant d' \leqslant d$; $k \geqslant 2d$.

Figure 1(a) is a 1-lattice structure diagram (where $k = 4, n = 20$). We add randomness to the structure diagram to get the small world diagram (Figure 1(b)). Given a coefficient ρ ($0 \leqslant \rho \leqslant 1$), we re-edit each edge in the 1-lattice structure diagram with a probability of ρ. We can keep the starting point of the edge to be edited unchanged, and then randomly select a node from other points as the end point of this edge. Each edge has ρ probability of being re-edited. ρ=0 indicate the initial structure diagram; ρ=1 indicates a completely random diagram; $0 < \rho < 1$ indicates a small world network diagram between the structure diagram and the random diagram.



(a) Ring lattice

(b) Small world

(c) Random

Fig 1. Comparison of three network structure diagrams
Source: Authors

After this re-editing, some "shortcuts" have emerged in the small world network diagram. The ratio of the number of shortcuts in a graph to the total number of edges reflects the degree of freedom of a graph. The small world model reflects its degree through the three parameters of clustering coefficient, feature length, and exponential feature length scaling ratio.

(1) Clustering coefficient: The clustering coefficient of a node y indicates the degree of interconnection between nodes connected with node y. It is defined as follows: the number of actually connected edges between nodes connected to y accounts for the proportion of all possible edges between these nodes. The clustering coefficient of a graph G is defined as the average value of the clustering coefficients of all nodes. which is:

$$C = \frac{1}{n}\sum_{i=1}^{n} \frac{2t_i}{k_i(k_i - 1)} \tag{3}$$

Where k_i is the degree of node i, t_i represents the number of connected edges between neighboring nodes of node i. In a network graph, each node has a shortest path with other nodes.

(2) Characteristic path length: the median value of the average of the shortest path length from all nodes to other nodes in the network. The feature length of a network graph is defined as the average feature length of the nodes in the graph. which is:

$$L = \frac{1}{n(n-1)/2} \sum_{1 \le i, j \le n} d(i, j) \tag{4}$$

Where $d(i, j)$ represents the number of edges included in the shortest path between any two nodes.

(3) Exponential feature length scaling ratio: the proportion of a network graph's feature length relative to the entire graph scale decreases exponentially.

If a network graph has the following characteristics, it shows the characteristics of a small world: high clustering coefficient, small feature length, and exponential feature length scaling ratio. The previous research work is based on a static network. In reality, the network, especially the Ad Hoc network, is mostly dynamic, and the relationship between the units in the dynamic network is changing at any time, not static. So we have to study how to find a shortest path between any two elements in a dynamic network.

III. Authentication routing protocol for wireless Ad Hoc network

In a real network, most nodes have fewer contact nodes, but a few nodes have more contact nodes. The previous research work assumes that every unit in the network is searchable, and its position in the network is unchanged, that is, a static network. In the wireless Ad Hoc network architecture in the 802.11 protocol [22], the relationship between dynamic network nodes changes at any time. As shown in Figure 2, when a node wants to communicate with another node, it must first broadcast routing information containing the IP address of the target node, and its neighbor nodes receive the information and then pass the information to their neighbor nodes [23]. Repeat this way until the information reaches the target node. This architecture requires that every node in the network can act as a router to determine the path that packets need to go through to reach their destination.

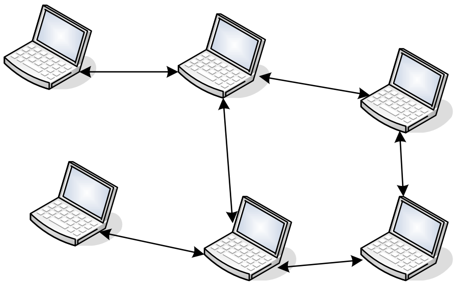


Fig. 2. Wireless Ad Hoc network architecture in 802.11 protocol

AODV protocol needs to broadcast routing messages many times, which brings a great burden to ad hoc network with limited resources, and it has no security mechanism of its own. Therefore, malicious nodes can launch multiple attacks. For example, a malicious node may impersonate some other nodes and forge a RREQ message to make it look like it was sent by the impersonating node. In addition, malicious nodes can also forward RREQ messages to them, not to increase the number of routing hops, but to reduce the number of hops. This causes the path passing through the malicious node to appear to be the shortest, so that all packets will pass through the malicious node when they are transmitted. In addition, a malicious node can also make itself pretend to be a destination node or pretend that it has a route to the destination node. In this way, it can then ensure that all messages sent to the destination node are sent to the malicious node by forging RREP messages. The schematic diagram of AODV routing protocol is shown in Figure 3, in which node A tries to find the route to node B.

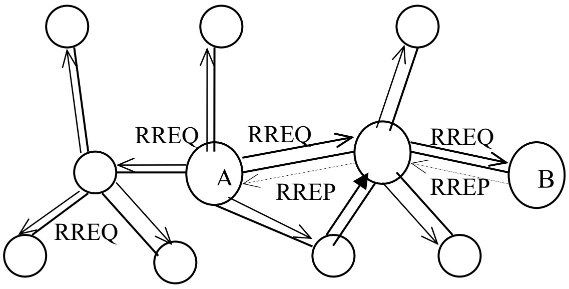


Fig. 3. AODV Routing Protocol

A. A small world model for Ad Hoc Networks

In a certain range of wireless ad hoc networks, the nodes often have the following characteristics:

(1) There is a high probability of connection between nodes with a relatively close regional distance. With the increase of regional distance, the probability of connection becomes smaller and smaller.

(2) Most of the nodes in the network have direct connections within a certain range.

(3) The connection between any two nodes is not always bidirectional in the network. For example, node A has the IP address of node B, or node A owns the public key of node B, but on the contrary, node B does not necessarily have the IP address or public key of node a at the same time. Let's set up a new small world model to reflect the relationship between these nodes. Figure 4 is a small world network with 20 nodes.

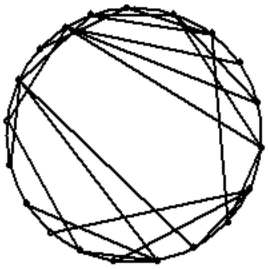


Fig. 4. Small world network diagram of ad hoc network nodes (|G|=20)

In the graph G of wireless ad hoc network, we use GR to represent the relationship set between two nodes. Let $<x,y>\in GR$ represents an edge of the graph, which denotes that node x has the IP address of y, and this relationship is not symmetric.

The number of nodes contained in network diagram G is recorded as |G|. The steps of constructing the small world network diagram of this new model are as follows:

Step1: Construct a basic struc ture diagram.

Suppose for a network graph G, each node in the network joins the nodes related to it in the following way:

For all $x \in G$

$$y_k \equiv (x-1+|G|)(\bmod |G|)$$

$$<x,y_k>\in GR$$

$$z_k \equiv (x+1+|G|)(\bmod |G|)$$

$$<x,z_k>\in GR$$

In the structure diagram, each node x has at least two relation nodes y_k and z_k, which ensures that there is a path between any two nodes of the model diagram.

Step2: Add random parameter.

Suppose the distance between two nodes x and y in the network is $d(x,y)=|x-y|$. We introduce a random parameter r to reflect the relationship between the distance between nodes and the probability with relation. The probability that node x has the IP address of node y is $p=d(x,y)^{-r}$. It can be seen that the distance between nodes is inversely proportional to the probability of their relationship. $p\_in(<x,y>,p)\in GR$ denotes that $<x,y>$ is added to the relation set GR with the probability of p. The way to add randomness is as follows:

```
For all $x \in G$
for $i=2$ to $\frac{|G|}{2}$
    $p=[d(x,y)^{-r}]$
    $p\_in(<x,y>,p)\in GR$
```

Step3: Add reciprocal coefficient.

A parameter s is called reciprocal coefficient which means that if node x has the IP address of node y, the probability that y also has the IP address of x is s. The way to join the reciprocal relationship is as follows:

```
For all $<x,y>\in GR$
if $<y,x>\notin GR$
    $p\_in(<y,x>,s)\in GR$
```

According to the above method of searching path, 10000 nodes are used for simulation experiment. When the random parameter $r=1.60$, the reciprocal coefficient $s=0.80$, and the characteristic length $L=9.106$ and the clustering coefficient $C=0.260$ are obtained. The smaller the distance between the nodes is, the more likely they are to have each other's IP address, which can ensure a higher clustering coefficient. Moreover, as the value of random index increases, the feature length also increases, but their proportion is relatively small compared with the number of nodes in the network. Therefore, it has the characteristics of small world network.

B. *Authenticated Routing Protocol for Wireless Ad Hoc Network*

We assume that each node has a trusted certificate server T to create certificates for them before joining the network, and then distribute the certificates. In order to verify the authenticity of each node certificate, all nodes in the network can obtain t's public key. The following is the certificate format for node A:

$$\mathrm{cert_A=PrK_T(IP_A,Puk_A,t,e)}$$

Where $\mathrm{IP_A}$ is the IP address of node A, $\mathrm{Puk_A}$ is the public key of node A, t is the time when the certificate was created, and e is the time the certificate expires, $\mathrm{PrK_T}(\cdot)$ represents an algorithm which denotes that the certificate was signed with T's private key.

When the node A wishes to find a path to node X, It will search according to the small world network model we established. First, it selects a node with the shortest path to node X as the intermediary, assuming s_1.The node A broadcasts a message called the route discovery packet (RDP) to s_1, which is similar to the AODV route request message. The RDP message has the following format:

$$\mathrm{\{PrK_A(RDP,IP_X,cert_A,N_A,t),IP_X\}}$$

Where the RDP message contains the certificate of node A and a Nonce value N_A (to prevent replay attack). When node a sends an RDP message, N_A is incremented once. $\mathrm{IP_X}$ represents the IP address of target node X. t represents the current time. $\mathrm{PrK_A}(\cdot)$ denotes that the certificate was signed with A's private key.

When another node s_1 receives the RDP message, it first extracts the public key of node A from the message certificate, and then verifies whether the signature is valid. Finally, node s_1 also checks whether the certificate has expired. Then it checks whether the node with the opposite IP address has the information of target X. If not, selects a node with the shortest path to the target X node in its relationship node as the mediation, assuming s_2.The node s_1 signs the message with its private key, and attaches its own certificate, then rebroadcasts the RDP message to its neighbor (node s_2) as follows:

$$\mathrm{\{PrK_{S_1}[PrK_A(RDP,IP_X,cert_A,N_A,t)],cert_{S_1},IP_X\}}$$

Note that node s_1 only adds its own certificate and signature to the RDP message, and does not modify it. When the next node (such as node s_2) receives the message, it adopts the same processing method. The format of the message processed by node s_2 is as follows:

$$\mathrm{\{PrK_{S_2}[PrK_A(RDP,IP_X,cert_A,N_A,t)],cert_{S_2},IP_X\}}$$

If it goes on like this，Assuming that node s_j was the last hop before node X, then node X sends to node s_j the following message：

$$\mathrm{PrK_X[REP,IP_A,cert_A,N_A,t]}$$

The field REP specifically indicates that this is a REP message. The message contains the IP address of node A, the certificate of node X, the random number sent by node A, and the time stamp sent by node A. Finally, node X also uses its private key to sign the message. Once the node s_j receives the REP message, it will verify the authenticity of the message, then sign the message and attach its own certificate, and finally send the updated message to the previous hop node s_{j-1}. Like the RDP message, the intermediate node deletes the signature and certificate of the previous intermediate node. At last, node A receives the REP. It verifies the authenticity of the response immediately. Finally, node A can obtain the target information in a short relationship chain, and establish the route to node X, and initiate a session with it.

IV. Performance Analysis

In this section, we optimize the route discovery and maintenance process of the proposed protocol, Then we use NS2 simulation software for simulation, analyze the simulation performance curve, and verify the feasibility and effectiveness of the scheme.

A. *Optimization of route discovery process*

There are already literatures that optimize the route discovery process [24, 25]. They limit the number of forwarding to within 6 hops, and intermediate nodes forward to all neighboring nodes when there is no route record. The study found that its exploration speed is still not fast enough, and the overhead of intermediate nodes forwarding to all neighboring nodes is relatively large. To solve this problem, we set a variable for the maximum number of retransmissions in the request packet. When we first started exploring, the variable was 3. In general, the destination node can be found up to 6 hops, and most destination nodes are concentrated in 3 to 6 hops, so it is reasonable to choose half of the maximum hops as the starting value. The advantage of this setting is that if the destination node is within 3 hops at a certain moment, you can quickly find the destination node, and you can quickly explore the route without having to explore beyond 3 hops. We regularly process each exploration initiated in the routing request table. If the route is not found within 3 hops after the validity time arrives, then we increase the value of the maximum number of forwarding times by 1 to re-initiate another exploration and reset the validity time of the request. We continue to conduct such layer-by-layer exploration. If the route is still not found after the maximum number of forwarding times reaches 6, then initiate the route exploration of the original AODV protocol, thus ensuring the final normal operation of the protocol.

B. *Simulation based on NS2 software*

NS2 (Network Simulator) is currently the most commonly used network simulation software. NS2 is a discrete event simulator with the characteristics of good openness, strong extensibility, and suitability for windows and linux system platforms. It is an excellent simulation tool for studying network topology and analyzing network transmission. We mainly use the following three indicators to analyze the routing protocol simulation results and estimate the performance of each protocol:

(1)Group delivery rate

The packet delivery rate is the ratio of the number of packets sent by the source application layer to the number of packets received by the destination node, and it reflects the maximum throughput supported by the network. It is an indicator of the completion and correctness of the routing protocol.

(2) Average end-to-end delay

The end-to-end average delay is calculated using the following formula, where N represents the number of all packets successfully received during the simulation, rt_i represents the time the i-th packet arrives at the destination, and st_i represents the time the i-th packet is sent. The smaller the delay, the faster the response and the more satisfactory the network quality.

$$\text{Average end-to-end delay} = \frac{1}{N}\sum_{i=1}^{N} rt_i - st_i \quad (5)$$

In the absence of attackers, we implement the simulation experiment of ARSW and SAODV. We assume that all nodes are loosely time synchronized and synchronization errors are fixed. In the simulation, the space of our simulation experiment is a rectangular area with an area of 1500m × 1000m and 50 nodes. The maximum end-to-end network delay is 0.1s, and the communication range of each node is set to 250m. There are 10 pairs of communication nodes. Each source sends 64 bytes of constant bit rate (CBR) traffic at the rate of 4 packets / second. The signature generation time is set to 10ms, and the signature verification time is set to 1ms. The time required to calculate the hash value is omitted in the simulation.

In the case of the same network topology and simulation parameters, the performances of ARSW and SAODV are compared. In order to maximize the advantages of SAODV, we simulate two versions of SAODV, namely cache enabled and cache disabled, and compare the following indicators with AODV and SAODV to evaluate the performance of packet delivery rate and packet delivery delay.

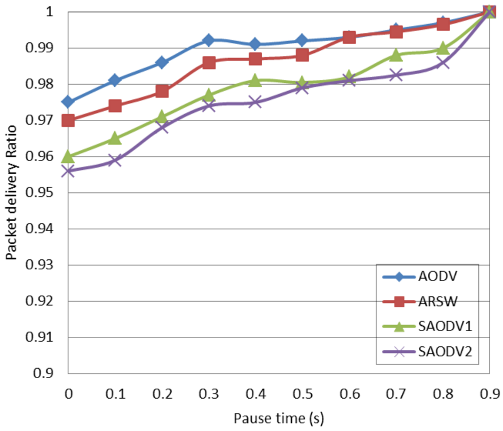


Fig. 5. Performance comparison: Packet Delivery Ratio

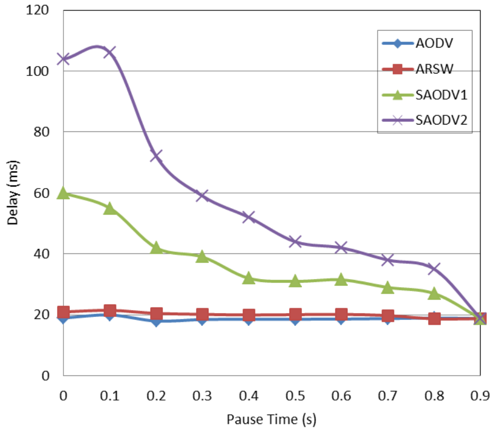


Fig. 6. Performance comparison: Packet Delivery Delay

The simulation results are shown in Figure 5 and figure 6, which are based on an average of more than 60 runs of different mobile files for each pause time. 95% confidence interval of the index is drawn as error line. During all pause times, the packet delivery rate of ARSW decreases by up to 1%, which shows that the performance of ARSW is better than that of two versions of SAODV. The packet delivery rate of a cached SAODV (SAODV 1) is better than that of a no cached SAODV (SAODV 2). Due to the increase of communication overhead, the average delay of packet transmission increases slightly, while the delay of SAODV increases about three times as much as when cache is enabled, and five times as much as when there is no cache support. In general, of all the performance indicators we studied, ARSW is better than two versions of SAODV.

V. Conclusion

Wireless ad hoc network has a wide range of application prospects. Different application requirements and application environment have different requirements for ad hoc network performance and corresponding network protocol. We use the relationship with each other's IP address information to build a new small world network model. We can quickly find the shortest path with a large probability in the small world model. This paper uses the advantage of small world model and combines the identity authentication mechanism to construct an authenticated routing protocol. Experimental results show that the protocol proposed in this paper can effectively improve the efficiency and security of self-organizing network communication. However, this scheme avoids the discussion of signature algorithm. How to build an efficient signature algorithm suitable for wireless ad hoc network is our further research problem.

REFERENCES

[1] Elizabeth M. Royer, Chai-Keong Toh. A review of current routing protocols for ad-hoc mobile wireless networks. IEEE Personal Communications, 6(2): 46-55, 1999.

[2] Jorge E. O. T., Molina J. L. B., Miguel A. S. L. Simulation and evaluation of ad hoc networks under different mobility models. Ingeniería E Investigación, 23(3): 44-50, 2003.

[3] Tianbo L., Hao C. Anonymous routing protocols for mobile ad-hoc networks. International Journal of Security and its Applications, 10(4): 229-240, 2016.

[4] Banala R., Sakthivel M. A review on delay-minimized routing protocol in mobile cognitive ad hoc networks. International Journal of Computer Sciences & Engineering, 6(7): 991-996, 2018.

[5] Prabhavat S. , Narongkhachavana W. , Thongthavorn T. , et al. Low Overhead Localized Routing in Mobile Ad Hoc Networks. Wireless Communications & Mobile Computing, 2019, 6(4): 1-15.

[6] Shanmugasundaram D. , Shanavas A. R. M. Avoidance Cosmic Dust implementing in Ad Hoc on-demand Distance Vector (CDA AODV) Routing Protocol[J]. International Journal of Computer Sciences & Engineering, 2019, 7(4): 995-1005.

[7] Kothandaraman D., Chellappan C., . Energy Efficient Node Rank-Based Routing Algorithm in Mobile Ad-Hoc Networks. International Journal of Computer Networks & Communications, 2019, 11(1):45-61.

[8] Shanmugasundaram D., Shanavas A. R. M. . Avoidance Cosmic Dust implementing in Ad Hoc on-demand Distance Vector (CDA AODV) Routing Protocol. International Journal of Computer Sciences & Engineering, 2019, 7(4):995-1005.

[9] Kim, C., Talipov, E., & Ahn, B. A reverse aodv routing protocol in ad hoc mobile networks. lecture notes in computer science, pp. 522-531. 2016.

[10] Navjot K., Ashok K., & Daviet J. (2011). Comparison and analysis of RREQ and RREP for dynamic wireless network. indian journal of computer science & engineering, 2(3), 73-78, 2011.

[11] Kargl F., Schlott S. & Weber M. (2004). Securing ad hoc routing protocols, Proceedings. 30th Euromicro Conference, 2004., Rennes, France, pp. 514-519.

[12] Kumar S., Dhull K., Sharma D., et al. Evaluation of AODV and DYMO Routing Protocol using Generic, Micaz and Micamotes Energy Conservation Models in AWSN with Static and Mobile Scenario[J]. Scalable Computing, 2019, 20(4):653-661.

[13] Watts D.J. & Strogatz S.H. (1998) , Collective dynamics of 'small-world' networks, Nature, 1998, 393(6684): 440–442.

[14] Qin Y , Guo D , Luo L , et al. Design and optimization of VLC based small-world data centers[J]. Frontiers of Computer Science in China, 2019, 13(5):1034-1047.

[15] Qiu T.p, Liu X., Li K., et al. Community-Aware Data Propagation with Small World Feature for Internet of Vehicles[J]. IEEE Communications Magazine, 2018, 56(1):86-91.

[16] Reka A., Hawoong J., & Albert-Laszlo B. Error and attack tolerance of complex networks. Nature. 406(6794):378-382, 2004.

[17] Guidoni, D. L. , Mini, R. A. F. , & Loureiro, A. A. F. On the design of resilient heterogeneous wireless sensor networks based on small world concepts. Computer networks, 54(8):1266-1281, 2009.

[18] Zhang, J. & Elkashlan M., A small world network model for energy efficient wireless networks, IEEE Communication. Lett., 17(10): 1928–1931, 2013.

[19] Zarepour, M., Universal and non-universal neural dynamics on small world connectomes: A finite-size scaling analysis. Physical Review E. 100(5):52138, 2019.

[20] Tefan G. Small directed strongly regular graphs. Algebra Colloquium, 27(1), 11-30, 2020.

[21] Zhang L. & Tang Y. Research on the method of improving network security based on small world model. 40(13):136-139, 2005.

[22] Oscar P. Sarmiento, F. G. Guerrero, D. R.(2008) Basic security measures for IEEE 802.11 wireless networks. Ingenieria E Investigación, 28(2):89-96. 2008.

[23] Wu J. &Yang S. Logarithmic Store-Carry-Forward Routing in Mobile Ad Hoc Networks. IEEE Trans. on Parallel and Distributed Systems, 18(6): 735-748, 2007.

[24] Anhong Zhong. Research on Mobile Ad Hoc Network Routing Protocol Based on Small World Theory [D]. Xidian University, 2011.

[25] Li Yong, Li Wei, Zhao Weiquan, Optimization for Dynamic Source Routing Based on the Small-world Theory [J], Computer Engineering, 2005 (9):102-104.