Transactions on Machine Intelligence 6(3) (2023) 137-145

ISSN Online: 2821-1693

Transactions on Machine Intelligence

Journal Homepage: https://tmachineintelligence.ir/index.php/TMI

A Security Method for Intrusion Detection in Mobile Ad Hoc Networks Based on DSR Protocol

S. Panahi[1], S. Jahanbakhsh Gudakahriz[2,*]

[1] MSc, Instructor, Department of Computer Engineering, Islamic Azad University, Ardabil, Iran
[2] Assistant Professor, Department of Computer Engineering, Islamic Azad University, Germi Branch, Germi, Iran

ARTICLE INFO

Article History:
Received 25 May 2023
Received in revised form 15 June 2023
Accepted 14 September 2023
Available online 15 September 2023

Keywords:
Mobile Ad Hoc Networks, Routing, Security, Intrusion Detection, DSR Protocol

ABSTRACT

A mobile ad hoc network consists of mobile nodes communicating with each other without centralized control or infrastructure. The inherent wireless nature of these networks introduces significant security challenges. However, recognizing that routing plays a pivotal role in most mobile ad hoc network operations, enhancing the security of routes can contribute to overall network performance. This paper introduces a novel technique aimed at improving intrusion detection in mobile ad hoc networks by identifying and detecting black hole nodes. The proposed solution involves the introduction of the S-DSR protocol, a variant of the DSR protocol. The primary objective is to enhance intrusion detection by identifying black hole nodes during the route detection phase and subsequently excluding routes containing them. This ensures secure data transmission and reception within the network. The protocol, named S-DSR, is designed to address these security concerns. The results obtained from simulations conducted in the NS-2 environment indicate that the S-DSR protocol outperforms the traditional DSR protocol in terms of network performance.

1. INTRODUCTION

Mobile ad hoc networks consist of temporary sets of mobile nodes that lack central management [1]. Consequently, routing protocols play a vital role in facilitating communication [2]. Thus, routing is a crucial concern in mobile ad hoc networks. Owing to the constant movement of nodes in these networks, the network structure is in a state of constant flux [3]. Thus, routing is a crucial concern in mobile ad hoc networks. Mobile ad hoc networks have garnered significant attention because of their advantages, including their lack of need for a predefined infrastructure or central management, and their high level of mobility and flexibility [4].

The use of mobile ad hoc networks (MANETs) is characterized by their infrastructure-less nature and self-organizing capabilities [5]. Configured routing algorithms are implemented in these networks to extend the communication range of nodes beyond a single step [6]. These algorithms possess the capability to establish a route even in the presence of dynamic network topologies [7]. As the nodes in such networks function as routers, these protocols exercise complete control over the data packets transmitted through them [5]. Security issues in ad hoc

* Corresponding Author: S. Jahanbakhsh Gudakahriz
Assistant Professor, Department of Computer Engineering, Islamic Azad University, Germi Branch, Germi, Iran

http://dx.doi.org/10.47176/TMI.2023.137

© 2023 by the authors. Licensee T.M.I, Tehran, Iran. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) license (http://creativecommons.org/licenses/by/4.0/).

networks encompass the lack of infrastructure or central control, making network management more difficult [8]. The trustworthiness of routing protocols is directly linked to the security level of these networks [5].

Due to the increasing significance of these networks, we have to propose optimal strategies to improve their Security. Intrusion detection systems are essential for securing computer networks by detecting subversions or abuses [9]. There are two approaches to detect abnormal behavior and abuse, depending on the type of analysis used in intrusion detection systems. Compared to abuse detection techniques, methods for identifying abnormal behavior demonstrate superiority, as altering attack patterns, which can be easily accomplished, will not result in detection errors [10]. A proposed approach by Tamilarasan et al. [11] evaluates sequential numbering differences of source and intermediate nodes when returning RREP.

A proposed approach by Tamilarasan et al. [11] evaluates sequential numbering differences of source and intermediate nodes when returning RREP. Typically, a malicious node's initial route response, as listed in the request/response table, will feature a higher destination sequence number. If the difference between the two is significantly high, the destination node is marked as malicious and removed from the request/response table. To determine if the destination node is indeed malicious, this method compares the source and destination sequence numbers. If the difference between the two is significantly high, the destination node is marked as malicious and removed from the request/response table. If the difference between the two is significantly high, the destination node is marked as malicious and removed from the request/response table. In a study by Rutvij et al. [12], various methods for detecting attacks in ad hoc networks were explored and a pertinent solution for mitigating such attacks was proposed. The method is adept at determining the optimal route and constructing a secure pathway to the destination node. Furthermore, this approach can effectively identify and eliminate malicious nodes, and can be successfully implemented in other routing protocols.

Gad, Nashat, and Barkat (2021) [13] proposed an intrusion detection system for Vehicular Ad Hoc Networks (VANETs) using machine learning, based on the ToN-IoT dataset. The researchers achieved promising results in terms of detecting and mitigating intrusion attempts in VANETs. Furthermore, Alkadi, Moustafa, Turnbull, and Choo (2021) [14] presented a deep blockchain framework-enabled collaborative intrusion detection method for protecting IoT and cloud networks. The researchers combined deep learning and blockchain to enhance the security of IoT and cloud networks, which may also be applicable to MANETs.

Srilakshmi, Alghamdi, Vuyyuru, Veeraiah, and Alotaibi (2022) [15] proposed a secure optimization routing algorithm for MANETs. The researchers developed an algorithm to optimize routing while addressing security concerns in MANETs. This approach provides a comprehensive method for enhancing the security of routing in MANETs, which is crucial for effectively detecting and preventing intrusions.

Mourad, Tout, Wahab, Otrok, and Dbouk (2021) [16] introduced the concept of Ad Hoc Vehicular Fog for enabling cooperative low-latency intrusion detection. The researchers leveraged fog computing to enable low-latency and cooperative intrusion detection in vehicular ad hoc environments. This approach may offer insights into utilizing fog computing for efficient intrusion detection in MANETs.

In another study, Jaisankar et al. [17] introduced a two-phase method for detecting black hole attacks, aimed to bolster security and intrusion detection. In the initial phase, RREP packets are updated with information regarding subsequent nodes. Prior to sending a packet, intermediate and destination nodes inspect the RREP packets. Suspicious nodes are logged in a "BIT" table by each node, listing the source and destination nodes, the current node, and details on the number of received, sent, and corrected packets. Suspicious nodes are logged in a "BIT" table by each node, listing the source and destination nodes, the current node, and details on the number of received, sent, and corrected packets. The corrected packet count in this table is updated, allowing for the identification of malicious nodes based on the number of packets they discard. Specifically, a node is deemed malicious if it receives packets from a source node without transmitting any to the destination node. Tamilselvan and Sankaranarayanan [18] proposed a dynamic approach for detecting black hole attacks in the context of routing and packet transmission. The method checks the destination serial number in RREP messages to detect attacks. The serial number of each node changes based on network traffic conditions in normal circumstances. With an increase in connections, the serial number value increases uniformly for each node, and it decreases uniformly when the number of connections reduces. However, if a point on the network is attacked, the value of the serial number increases significantly,

regardless of environmental conditions or network traffic volume. Deng et al. [19] propose using a resend request packet (FREQ) as an alternative approach. In this method, the intermediary node attaches information about the next hop towards the destination to the PREP packet when responding to the RREQ. Then, the source node sends a request for retransmission to the next hop of the responding node. The responding node, in turn, sends a route to the destination.

A new security approach for detecting intrusions in ad hoc networks using intrusion detection systems based on the DSR protocol is proposed in this paper. The DSR protocol is introduced in Section 2 to support the proposal. Section 3 contains the particulars of the proposed plan and Section 4 presents the results of the simulation. Finally, Section 5 provides a conclusion to the study.

2. DSR ROUTING PROTOCOL

In the DSR protocol (Dynamic Source Routing) [20], the source node generates a packet called "RREQ" that indicates the source and destination nodes when a node desires to connect to another node. The source node broadcasts the packet using a flood algorithm [21]. If a node receives an RREQ packet but does not recognize the destination route, it adds its name to the packet's list and broadcasts it. When the packet arrives at the destination, it will contain information about route nodes and their order. The destination node then generates an RREP packet, using the list provided in the header of the RREQ packet, and returns it. Intermediary nodes use the available list to determine where to send the packet. The packet will travel in a reverse fashion along the route until it reaches the source node. While this technique is effective and can reliably produce a solution, it also leads to an increase in network traffic and the consumption of high bandwidth due to the transmission of packets with large headers across the network. Additionally, as the distance between the source and destination nodes increases, the acceleration of header volume also increases. This is attributable to the inclusion of intermediary network element names in the packet's header. The data transmitter can include the destination route in the data packet header, enabling intermediary nodes on the route to identify the recipient of the packet. This algorithm is known as dynamic source routing.

If a node fails to transmit a data packet to the next node, it generates an RERR packet and sends it back on the route. Thus, the nodes that receive the RERR signal detect a connection interruption between them. Consequently, the routing process begins again.

An example of route failure is illustrated in Figure 1. Initially, a route is established between the source and the destination. However, over time, changes in the network's topology cause the route to fail as node a moves out of the radio range of node s. Subsequently, the previously identified route becomes unusable. To prevent such situations, stable routing is necessary, ensuring that identified routes remain functional for an extended period.

In the DSR request-based routing protocol, each node tries to shorten the route by entering an irregular state and listening to its neighbor's transmitted packets to eliminate unnecessary nodes. However, when additional nodes enter the irregular state and listen to all transmitted packets, it results in a large energy usage and processing overhead.

In the DSR protocol, when nodes enter the irregular state, they dynamically listen to packets transmitted by neighboring nodes to shorten active routes. However, this causes increased overhead and energy consumption as the nodes listen to all packets from the neighboring nodes.

3. THE PROPOSED PROTOCOL

Security is a significant challenge in ad hoc networks due to the potential for security issues such as eavesdropping, data tampering during transmission, falsifying individuals' identification, and disrupted routing operations. These issues are in addition to the usual complications present in wired networks. Furthermore, the lack of infrastructure for distributing encryption keys makes it impossible to rely on encryption. One of the crucial security concerns in ad hoc networks is introducing a secure routing algorithm for the network [22].

While the DSR protocol does not require frequent updates and incurs relatively low control overheads, it is only effective for networks containing fewer than 200 nodes, and nodes should not surpass a predefined speed threshold.

Additionally, flood diffusion can result in interference within the network. Using a cache to store identified routes can decrease the overhead of routing. In the DSR protocol, every data packet has to carry the complete route information, which leads to an increase in bandwidth usage. However, using a cache can lead to intermediary nodes transmitting outdated and invalid routes in the RREP packet to the transmitter. As a result, it is possible to come across an invalid or insecure route while attempting to identify routes. To address this issue, our proposed method aims to resolve such situations.

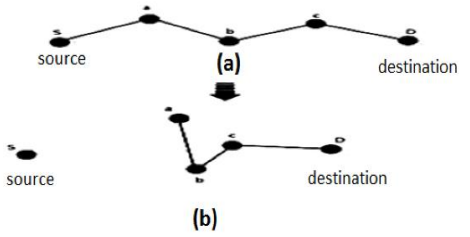

Fig. 1. (a) Initial Created Route, (b) Non-Optimality of the Route after the Movement of Nodes

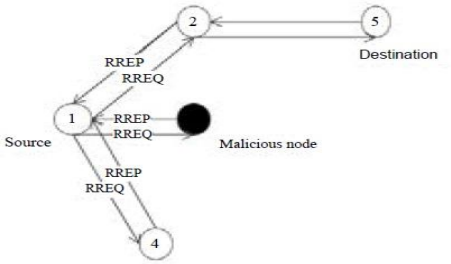

Fig. 2. An Example of Black Hole Attack in Mobile Ad Hoc Networks

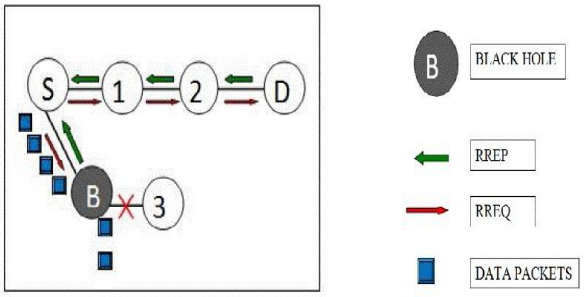

Fig. 3. Intrusion Detection Using the Proposed Intrusion Detection System

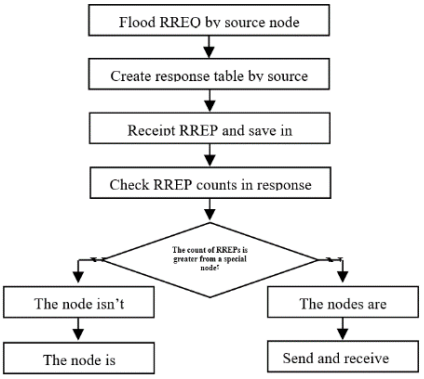

Fig. 4. The Flowchart of Proposed Intrusion Detection System

Given the security weaknesses enumerated above with regards to the DSR protocol, the proposed method tries to improve the security of this protocol. The proposed method is divided into the following two phases:

1. Checking control messages sent and received by the source and destination nodes which are searching for a route.
2. Evaluating the number of route request reply packets (RREP) reached the source node in the first phase.

3.1. First Phase

The proposed methodology entails monitoring all control packets, including route requests and request replies, transmitted and received between source and destination nodes. During this phase, a "reply table" is established, recording all received route reply packets (RREP), i.e., route reply packet specs. In this phase, the black hole node sends a route reply message containing the maximum serial number to represent itself as the destination node, prompting the source node to send transmitted packets to the black hole node. To prevent this from occurring, we established a reply table during this phase. Before sending information from the source node, we increase the expected wait time for a response to route requests in order to receive more request reply packets. This wait time is set to twice the usual time. Additionally, upon receiving the route request reply packets, we record the serial number of the packets and their transmission time in the reply table.

3.2. Second Phase

When the source node receives the RREP packet for the route request, it logs the destination's serial number and receiving time in the reply table during the first phase. Once the waiting period for the route request reply has ended, the proposed method will assess how many RREP packets have been saved in the table. If an individual node sends more than one route request reply packet (RREP), it is classified as a black hole node. However, if only one route request packet is sent from an individual node, that node can be trusted and considered one of the primary elements in the network. Receiving multiple route request replies from a node indicates that the node has falsely set its serial number to the maximum possible value to imitate the destination node. After identifying a compromised node, it will be isolated. Its specifications will then be sent to all trustworthy nodes on the network to ensure secure transmission, preventing data from being sent to the compromised node. In instances of black hole attacks, malicious nodes broadcast a falsified route as the shortest route to the destination. This allows the node to receive data sent by the source node, alter it, and subsequently drop it rather than deliver it. Figure 2 illustrates a black hole attack, where the malicious node (black hole) masquerades as Node 5 (destination) and collects data from Node 1 (source) that is meant for the destination node, subsequently destroying it.

The process pertaining to the proposed method is illustrated in Figure 3. According to this illustration, when nodes desire to transmit data packets to the Node D destination, they begin the route detection process. Upon receiving the RREQ packets, the malevolent Node B, also known as the black hole, declares having the shortest route to the destination, leading the source node to assume that the route detection process is finished and dismissing all other RREP messages. The source node sends packets to the malicious node, which can be readily destroyed by the black hole node (Node B) or sent to an unauthorized destination. In the proposed method, the route reply table comprises replies from various nodes, enabling the identification of Node B as the black hole node, and preventing data from being sent to it. Please refer to Figure 4 for the flowchart of the proposed intrusion detection system.

4. EVALUATING EFFICIENCY OF THE PROPOSED METHOD

In order to evaluate the proposed method, the changes mentioned above are applied on the DSR protocol in NS-2 simulation environment and it will be compared to the base protocol with regards to various efficiency criteria under different scenarios. In this simulation the measures of evaluating efficiency include: packet delivery ratio, average end to end delay, and number of dropped packets. The new protocol is called S-DSR which is compared to the base protocol i.e. the DSR protocol.

4.1. THE FIRST SIMULATION SCENARIO

In this scenario, the number of nodes is considered as variable in order to evaluate the efficiency of the protocol under various conditions of network density. The results of the simulation are presented in figures 5 to 7.

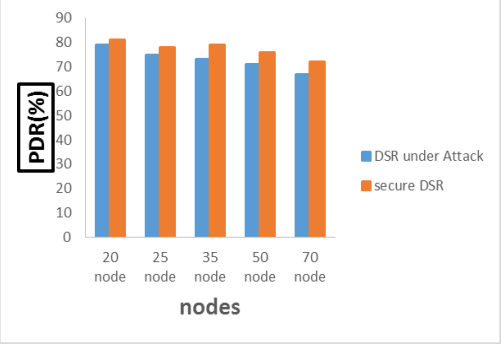

Fig. 5. Packet Delivery Ratio versus Number of Nodes

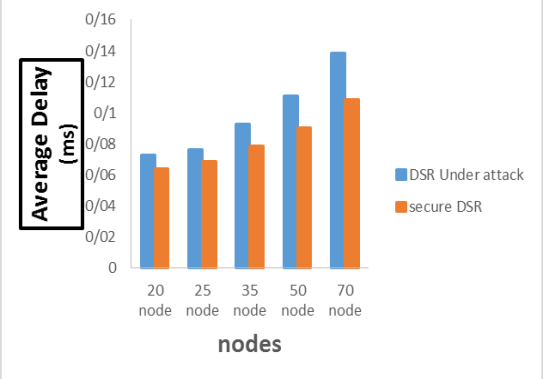

Fig. 6. End to End Delay versus Number of Nodes

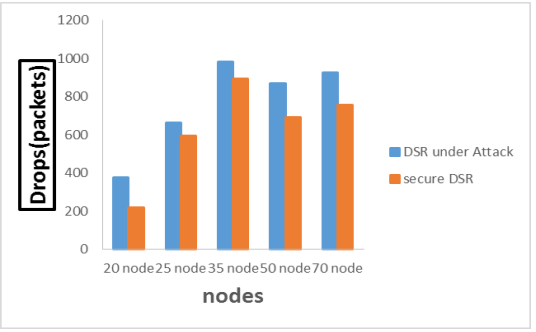

Fig. 7. The Number of Dropped Packets versus Number of Nodes

Based on the results shown in Figure 5, which display the packet delivery ratio versus the number of nodes, it is evident that the secure DSR performed significantly better in detecting this parameter under all simulation conditions, compared to DSR under attack. These findings highlight the superior efficiency of the proposed system in detecting attacks or intrusions. The improved performance is attributed to the utilization of the reply table and the recording of relevant parameters, such as the waiting time, in the table. The optimal state for this simulation is achieved when there are 20 nodes on the network. Figure 6 illustrates that the end-to-end delay decreases significantly for secure DSR compared to DSR under attack across all simulation conditions. This phenomenon can be attributed to the proposed method for attack detection. According to Figure 7, the relationship between the number of nodes and dropped packets indicates that this parameter is greatly minimized in secure DSR, as compared to DSR under attack in all simulation conditions. The network's performance improves with reduced lost packets. However, the number of lost packets intensifies with an increase in the number of network nodes. However, the number of lost packets intensifies with an increase in the number of network nodes. However, the number of lost packets intensifies with an increase in the number of network nodes. This pattern is also evident in this simulation.

4.2. The Second Simulation Scenario

In this scenario, the speed of the nodes is considered variable in order to be able to evaluate the efficiency of the protocol under various states of network dynamics. The parameters set for this scenario are presented in Table 1. The results of the simulation are presented in Figures 8 to 10.

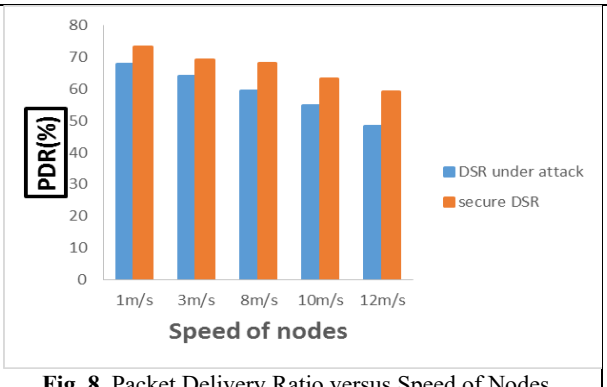

Fig. 8. Packet Delivery Ratio versus Speed of Nodes

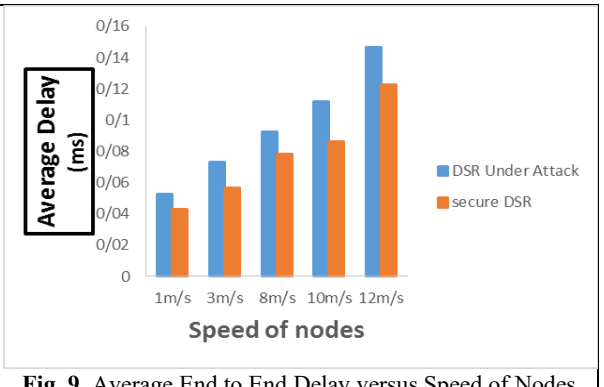

Fig. 9. Average End to End Delay versus Speed of Nodes

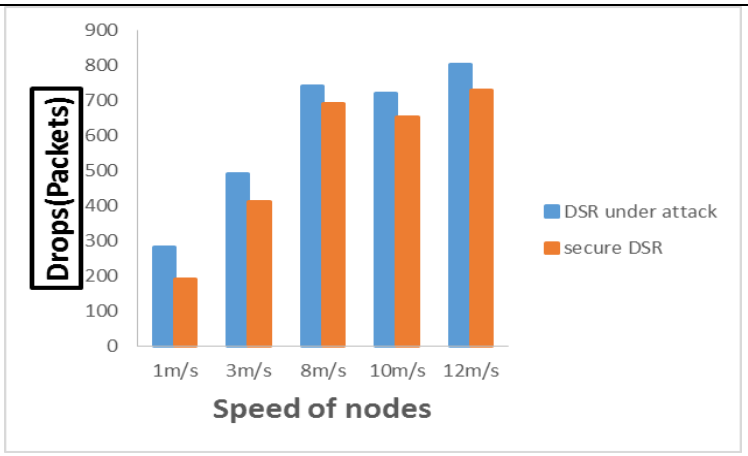

Fig. 10. Number of Dropped Packets versus Speed of Node

Table 1. Parameters for the Second Scenario

Parameters	Values of parameters
Environment	500 m × 500 m
Number of nodes	40
Routing protocol	DSR, S-DSR
Transmission range	250 m
Simulation times	800 s
MAC layer	802.11
Type of traffic	CBR (UDP)
Buffer size	50 packets
Node pause time	0 seconds
Number of malicious nodes	1
Speeds of nodes	1, 3, 8, 10, 12 m/s
Location of nodes	Random

According to Figure 8, the use of the proposed intrusion detection method in the network resulted in an increase in the packet delivery ratio relative to the DSR protocol under attack. This improvement in service quality indicates better network performance compared to the under attack condition. The optimal packet delivery value in this simulation occurs at a speed of 1 m/s. This is due to the network topology remaining relatively constant, resulting in fewer link deteriorations.

Figure 9 demonstrates that the end-to-end delay in the proposed method is significantly lower than that of DSR under attack conditions across all simulation scenarios. The proposed method is utilized for detecting and eliminating the malicious black hole node. It is observed that the optimal delay time is achieved at a speed of 12 m/s, demonstrating that higher node speeds result in increased end-to-end delay as links between nodes deteriorate rapidly.

Figure 10 displays a reduction in the number of dropped packets versus node speed when using the proposed method compared to the DSR protocol under attack. This chart demonstrates that implementing the intrusion detection system and employing the technique of recording the serial number of the destination node and waiting time in the reply table to assess the source and destination nodes' normal or malicious state results in fewer lost packets.

5. CONCLUSIONS

Given the importance of routing security in mobile ad hoc networks, this paper proposes a secure protocol that modifies the DSR routing protocol. The protocol detects routes that contain black hole nodes during the route identification process and removes these routes from consideration by nodes. To evaluate the effectiveness of this approach, we conducted several simulations within the NS-2 simulation environment. The S-DSR protocol was compared to the DSR base protocol in simulations. The results demonstrate superior performance of the S-DSR protocol compared to the base protocol. Similar mechanisms can be applied in future studies to develop new secure methods for mobile ad hoc networks.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] Krishnan, R. S., Julie, E. G., Robinson, Y. H., Kumar, R., Son, L. H., Tuan, T. A., & Long, H. V. (2020). Modified zone based intrusion detection system for security enhancement in mobile ad hoc networks. Wireless Networks, 26(2), 1275–1289. doi:10.1007/s11276-019-02151-y

[2] Khezri, E., & Zeinali, E. (2021). A review on highway routing protocols in vehicular ad hoc networks. SN Computer Science, 2(2). doi:10.1007/s42979-021-00451-9

[3] Ferreira, M. A., Lukkarinen, J., Nota, A., & Vel'azquez, J. J. L. (2022). Non-power law constant flux solutions for the Smoluchowski coagulation equation.

[4] Uddin, L. (2021). Cognitive and behavioural flexibility: neural mechanisms and clinical considerations.

[5] Rao, P. C. S., Lalwani, P., Banka, H., & Rao, G. S. N. (2021). Competitive swarm optimization based unequal clustering and routing algorithms (CSO-UCRA) for wireless sensor networks. Multimedia Tools and Applications, 80(17), 26093–26119. doi:10.1007/s11042-021-10901-4

[6] Srilakshmi, U., Alghamdi, S. A., Vuyyuru, V. A., Veeraiah, N., & Alotaibi, Y. (2022). A secure optimization routing algorithm for mobile ad hoc networks. IEEE Access: Practical Innovations, Open Solutions, 10, 14260–14269. doi:10.1109/access.2022.3144679

[7] Saboksayr, S. S., & Mateos, G. (2023, June 4). Dual-based online learning of dynamic network topologies. ICASSP 2023 - 2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). Presented at the ICASSP 2023 - 2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Rhodes Island, Greece. doi:10.1109/icassp49357.2023.10096392

[8] Subhrahmanyam, G., & Ginimav, I. (2019). Intelligent Routing Mechanisms in IoT. Intelligent System and Computing.

[9] Zipperle, M., Gottwalt, F., Chang, E., & Dillon, T. (2023). Provenance-based Intrusion Detection Systems: A survey. ACM Computing Surveys, 55(7), 1–36. doi:10.1145/3539605

[10] Kanakogi, K., Washizaki, H., Fukazawa, Y., Ogata, S., Okubo, T., Kato, T., Yoshioka, N. (2022). Comparative evaluation of NLP-based approaches for linking CAPEC attack patterns from CVE vulnerability information. Applied Sciences (Basel, Switzerland), 12(7), 3400. doi:10.3390/app12073400

[11] Tamilarasan, S. (2014). Securing AODV Routing Protocol from Black Hole Attack. International Journal of Computer Science and Telecommunications, 52–56.

[12] Rutvij, H., & Sankita, J. (2016). DoS Attacks in Mobile Ad-hoc Networks: A Survey.Second International Conference on Advanced Computing & Communication Technologies. 535–540.

[13] Gad, A. R., Nashat, A. A., & Barkat, T. M. (2021). Intrusion detection system using machine learning for vehicular ad hoc networks based on ToN-IoT dataset. IEEE Access: Practical Innovations, Open Solutions, 9, 142206–142217. doi:10.1109/access.2021.3120626

[14] Alkadi, O., Moustafa, N., Turnbull, B., & Choo, K.-K. R. (2021). A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks. IEEE Internet of Things Journal, 8(12), 9463–9472. doi:10.1109/jiot.2020.2996590

[15] Srilakshmi, U., Alghamdi, S. A., Vuyyuru, V. A., Veeraiah, N., & Alotaibi, Y. (2022). A secure optimization routing algorithm for mobile ad hoc networks. IEEE Access: Practical Innovations, Open Solutions, 10, 14260–14269. doi:10.1109/access.2022.3144679

[16] Mourad, A., Tout, H., Wahab, O. A., Otrok, H., & Dbouk, T. (2021). ad hoc vehicular fog enabling cooperative low-latency intrusion detection. IEEE Internet of Things Journal, 8(2), 829–843. doi:10.1109/jiot.2020.3008488

[17] Jaisankar, N., Saravanan, R., & Swamy, K. D. (2010). A novel security approach for detecting black hole attack in MANET. In Communications in Computer and Information Science. Communications in Computer and Information Science (pp. 217–223). doi:10.1007/978-3-642-12214-9_36

[18] Tamilselvan, L., & Sankaranarayanan, V. (2008). Prevention of co-operative black hole attack in MANET. Journal of Networks, 3(5). doi:10.4304/jnw.3.5.13-20

[19] Deng, H., Li, W., & Agrawal, D. P. (2002). Routing security in wireless ad hoc networks. IEEE Communications Magazine, 40(10), 70–75. doi:10.1109/mcom.2002.1039859

[20] Zarzoor, A. R. (2021, September 18). Enhancing dynamic source routing (DSR) protocol performance based on link quality metrics. 2021 International Seminar on Application for Technology of Information and Communication (iSemantic). Presented at the 2021 International Seminar on Application for Technology of Information and Communication (iSemantic), Semarangin, Indonesia. doi:10.1109/isemantic52711.2021.9573233

[21] Samantaray, S., Sahoo, P., Sahoo, A., & Satapathy, D. P. (2023). Flood discharge prediction using improved ANFIS model combined with hybrid particle swarm optimisation and slime mould algorithm. Environmental Science and Pollution Research International, 30(35), 83845–83872. doi:10.1007/s11356-023-27844-y

[22] Al-Shareeda, M. A., Anbar, M., Hasbullah, I. H., & Manickam, S. (2021). Survey of Authentication and Privacy Schemes in Vehicular ad hoc Networks. IEEE Sensors Journal, 21(2), 2422–2433. doi:10.1109/jsen.2020.3021731