International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

IJISAE

ISSN:2147-6799 www.ijisae.org Original Research Paper

An Secured Intrusion Detection System Integrated with the Conditional Random Field For the Manet Network

Burhan R Rexhepi[1], Avneesh Kumar[2], M.S. Gowtham[3], R Rajalakshmi[4], Ms. Divya Paikaray[5], Pronab Kumar Adhikari[6]

Submitted: 03/11/2022 **Revised:** 12/01/2023 **Accepted:** 03/02/2023

Abstract MANET is a wireless network that lacks infrastructural support. Most operations they perform are coordinated between nodes because of their limited transmission range. Assess the secure MANET routing protocol in a malicious environment. However, in the MANET environment security is an important constraint that affects the data transmission rate and cause data loss. This paper developed an Intrusion Detection System Conditional RandomField (IDS – CRF) model for security. The developed model uses the hashing function integrated with the Conditional Random Field model. The IDS – CRF model uses the label sequences for data security in the MANET environment. The model uses the DSR protocol with the discriminative field to process the secure data in the MANET. The proposed IDS-CRF model uses the hashing function for improved data transmission security in the MANET environment. The performance of the proposed IDS – CRF model is comparatively examined with the conventional DSR protocol. The comparative analysis expressed that the proposed IDS – CRF model achieves the ~4% reduction in the delay and ~2% reduction in the routing overhead. Similarly, the proposed IDS – CRF model achieves the ~4% reduced energy consumption. In terms of the Packet delivery ratio and throughput the proposed IDS – CRF model achieves the ~4% - ~6% improved performance than DSR model.

Keywords*:Conventional Random Field, Intrusion Detection System, MANET, Security, DSR protocol.*

1. Introduction

A MANET is a wireless network consisting of clusters of wireless devices which are connected dynamically via wireless links to transmit information [1]. Personal computers (such as laptops and desktops, mobile phones or other types of mobile or wireless communication devices) can form wireless nodes. Any device that uses air as a medium for transmitting information can form a wireless node in MANET. These nodes can be physically connected to airplanes, vehicles, or people to enable communication between them [2]. The mobile node can serve as a router, receiver or sender. Whenever node serve as router, it receives data packets and transmits them to neighboring node, thus forwarding it to target node [3]. The router moves freely and organizes itself in a random manner; thereby quickly changing the topology of any wireless network in an unpredictable way. Such networks operate using independent strategies, or they can be part of a larger Internet. MANET is not safe due to its dynamic nature. Therefore, it is significant to be careful about the data sent through MANET [4].

Compared to the fixed-cable networks, wireless networks tend to get affected by the threats of physical security more often [5]. Careful consideration is needed for attacks like DoS, Spoofing and eavesdropping, which frequently occurs in a MANET [6]. In MANET, network control is decentralized in nature, which is a benefit when compared with the approaches that are centralized in nature. This is because the robustness of a decentralised system is comparatively higher than the centralized approaches [7]. This makes the system vulnerable to multiple threats. The central authority distributes keys to include security elements in infrastructure-based systems [8]. In a self-organizing network, solutions based on cryptography must include a method of distributing keys in a distributed way. In MANET, even if the quality of the decision-making process is decentralized, all nodes present in it must

[1] Accounting Lecturer, MBE, UBT College - Higher Education Institution.
bulikont@hotmail.com
[2] Professor, Department of Computer Application,Galgotias University, Greater Noida, Uttar Pradesh, India.
avneesh.avn119@gmail.com,
0000-0001-5860-3689
[3] Associate professor, ECE, Karpagam institute of technology, Coimbatore, Tamil Nadu, India.
gowtham.ece@karpagamtech.ac.in
0000-0003-1300-7183
[4] ECE, Panimalar engineering College, Chennai, Tamil Nadu, India.
rajeeramanathan@gmail.com
0000-0002-4399-4071
[5] Assistant Professor, School of Engg.&IT, ARKA JAIN University, Jamshedpur, Jharkhand, India.
divya.p@arkajainuniversity.ac.in
0000-0001-7886-1538
[6] Assistant Professor, (Ajay Kumar Garg Engineering College, Ghaziabad), India.
pthepronab@gmail.com

cooperate and participate [9].Security is an important issue in every field. However, up to date adequate study have not been carried out on the security issues of the MANETs [10].

This paper presented a security protocol for the MANET with the DSR routing model. The proposed IDS – CRF model uses the conditional random field model for the security improvement in the MANET. The proposed IDS-CRF model uses the conventional DSR protocol model for the examination. The comparative analysis expressed that proposed IDS – CRF model achieves the improved performance than the conventional DSR model.

2. Related Works

MANET consists of several communicating mobile nodes. As far as an access point is concerned, it has no fixed infrastructure. Although MANET has many advantages over traditional wired networks, they also face challenges in establishing secure communications. Mobile nodes that do not have any necessary security in MANET are vulnerable to threats. In addition, static configurations may not be suitable for topologies, which will constantly change based on security solutions.In [11] evaluated the MANET in terms of parameters, applications, services, attacks, and challenges. The author discusses five important security services, namely availability, identity verification, data integrity, nonrepudiation and confidentiality. They discussed important parameters in MANET security, such as network overhead, processing time, and energy consumption. Four MANET applications were discussed, namely commercial sector, military battlefield, local level and personal area network (PAN). In addition, security attacks in MANET are discussed, including internal and external attacks. It is pointed out that with the development of time, security attacks are constantly updated.

In [12] proposed a technique that provides data security for the network to use node authentication and digital signatures. The author discusses some previous methods for identifying malicious nodes. It was found that there is currently no way to provide identity verification for a new node before it joins the network. Therefore, the author proposeed a novel security mechanism called the use of node authentication (SMDNA) to protect MANET data. This mechanism uses AES and digital signatures to provide integrity, non-repudiation, identity verification, and confidentiality.

In [13] reviewed security challenges, security objectives, and various attacks on MANET. The author also proposes a solution that uses reactive routing protocols to address various security threats facing different layers. Based on their implementation and security, reactive protocols like DSR, AODV, and Temporary Ordered Routing (TORA) are discussed. In [14] proposes a black hole attack recognition technology that modifies the AODV routing protocol by adopting a biologicallyinspired optimization scheme (called the ant colony optimization (ACO) scheme) in MANET. By using the forwarding ratio at the node, each ant located at each node is used to calculate its pheromone value. The proposed protocol can improve security and performance, but this method can only detect one attack and is effective against black holes.

In [15] proposed WNTFLEPPROTOCOL, which reduces control packets and increases the packet delivery count received at the destination. The detection and elimination of worm nodes on the path during the path establishment process can minimize the loss of data packets and ensure the establishment of the network, as well as protect the data security through the Twofish algorithm. [16] proposed a security mechanism for MANET in DDoS (Distributed Denial of Service). Due to the limitation of routing protocols, various DoS attacks may occur in MANET. Nodes with abnormal MANET behavior identified through this active scheme also prevent DoS attacks through this method. Compared with other existing methods, this solution can provide better performance. By transferring the responsibility of this technology to neighboring nodes, the node parameters affected by this can be monitored.

The research findings on the security issues of using IDS for wormhole attacks, including anomaly-based IDS and norm-based IDS. Various researches on detection techniques for session hijacking attacks and erroneous data injection attacks are discussed. The proposed work aims to analyze the vulnerabilities and attacks in MANET and the detection technology of MANET. It is found from the literature that the DSR routing protocol uses a reactive method, aiming to eliminate the requirement of flooding the network periodically with messages updated in the table required by the table-driven method. Intermediate nodes also effectively use routing cache information to minimize overhead. Considering the advantages of DSR, this study uses DSR for solving the MANET data transmission security problem. When using the DSR protocol, the security of MANET will be improved, and the QoS will also be improved, including parameters such as routing overhead, PDR, throughput, end-to-end delay, and energy spent. The research can be used for communications applications in military support.

3. Dynamic Random Field Algorithm for MANET IDS-CRF

As the developed IDS – CRF mode uses the conventional Dynamic Secure Source Routing Protocol MANET reactive routing protocol. When the source node’s route cache does not contain the destination node, the data packets will be buffered and a route request (RREQ) will be broadcasted into the network. The intermediate DSR nodes will broadcast the RREQ to the desired sink node. Route Reply (RREP) message sent by the destination node on the reverse route back over the source node. Still, there were some security issues in the DSR protocol so, a novel Dynamic Source Secure Routing (DSSR) Protocol is proposed with the help of DSR protocol. It is a secure protocol with Digital signatures and DYDOG mechanism integrated with two fish algorithm.

Algorithm 1: MANET security with IDS – CRF

S means sender node, RREQ is route request, RREQn means route request for n nodes

```
1.if (the entry of routing is NULL for S) then
    2. if (2Hop is valid) then
        3. Formulate the  RENTRY
        4. state ←Transistent value
        5. Transmit RREQ
    6. else
        7. eliminate RREQ
    8. end if
9. else
    10. if (id of RREQ, SEQ_No, validate the hop) then
        11. for (entries the routing table)
            12. if (RREQ_Hop == RENTRYto HOP count) then
                13. if (RREQ_Metric < RENTRY_Value) then
                    14. update (ENTRY→ RREQn)
                15. else
                    16. eliminate RREQn
                17. end if
            18. else
                19. if (RREQ_HOP == (RENTRY |HOP)) then
                    20. update (RENTRY →RREQ)
                    21. state → stable state value
                22. else
                    23. update (RENTRY →  (RENTRY))
                    24. state → stable
                25. end if
            26. else
                27. Formulate the route entry for RREQn
                28. state → transient
                29. broadcast RREQ
            30. end if
    31. else
        32. remove RREQn
    33. end if
33. end if
```

To obtain an Authentication message, digital signature techniques used and Digital signature schemes contain two schemes, namely, Digital signature with an appendix, and a Digital signature with message recovery. Two-fish is a 128bit block cipher which accepts variable key up to 256 bits. This algorithm is used for the encryption process, which hides information within another.A new technique called DSSR protocol is introduced. This protocol is dependent on packets that are acknowledged. And hence it involves in finding the attacking packets in network by Digital Signatures. This method is compared with the IDS - CRF protocol by the following parameters PDR, Energy spent, Delay, throughput and routing overhead. From this, the delay, energy, and routing overhead will decrease and PDR, throughput will increase by a proposed DSSR algorithm.

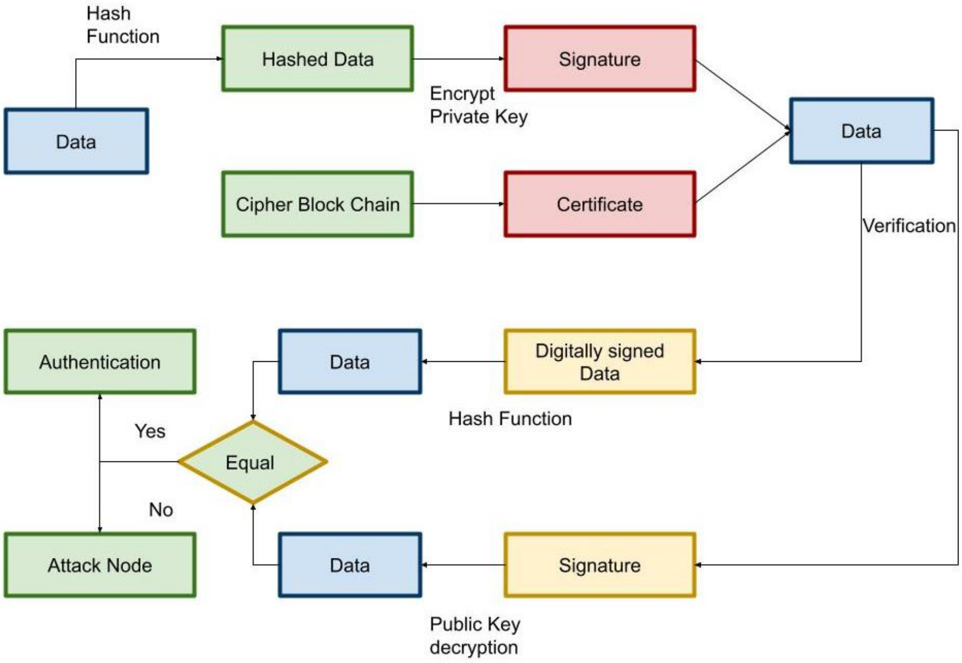


Fig. 1: Flow chart of IDS - CRF

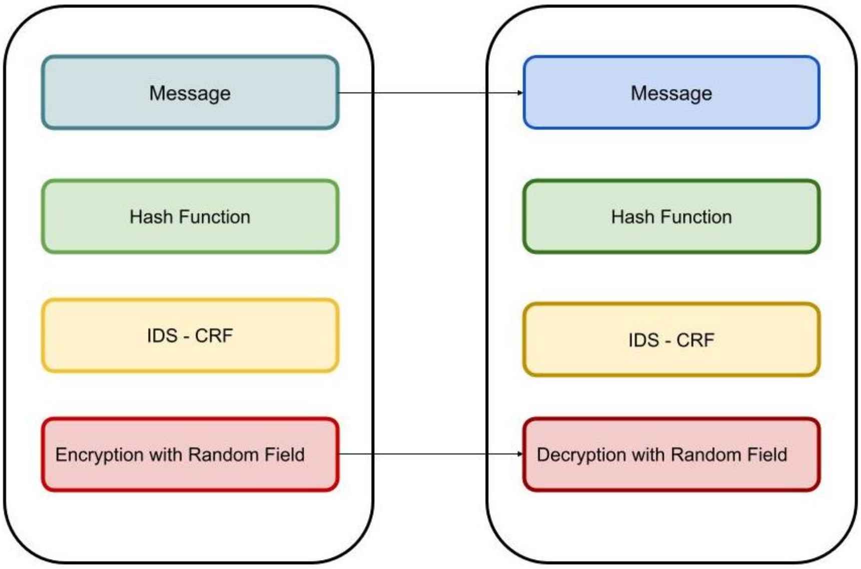


Fig. 2: Message Flow in IDS - CRF

4. Simulation Setting

The parameters considered for simulation are presented in Table 1. Then the performance measures, namely, routing overhead, Packet Delivery Ratio (PDR), end-end delay,throughput, and energy spent, are estimated in NS-2 environment. The table makes it clear that the number of nodes considered for the implementation is 50, and size of the packet is 500 bytes. The time taken for the process of simulation is 10 seconds. And the protocol used application layer is the User Datagram Protocol (UDP).

Table 1: Simulation Setting

PARAMETERS	VALUES
Number of nodes	50
Packet Size (Bytes)	500
Routing Protocol	DSR,IDS -CRF
Simulation Time (s)	10
Simulation Area (m)	500*500
Application Protocol	UDP

The MANET deployment in the simulation software with the implemented IDS – CRF model is presented in the figure 3.

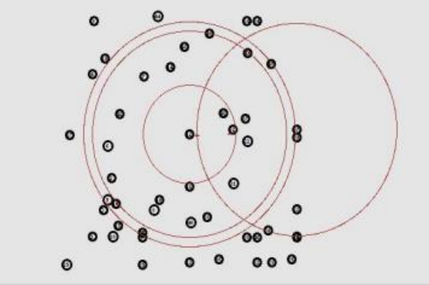


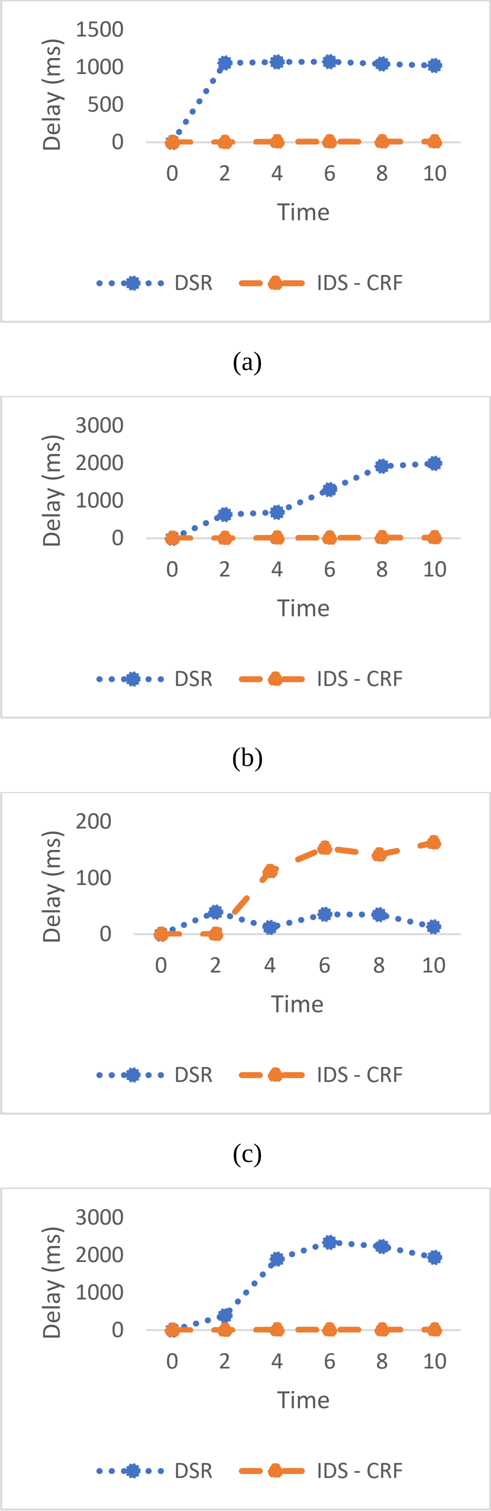
Fig. 3: MANET Deployment

The table 2 provides the comparative analysis of the proposed IDS – CRF model and the DSR protocol under the different attack scenario is presented.

Table 2: Comparison of Simulation parameters

	DSR						IDS-CRF					
	Time	**Delay**	**Energy**	**PDR**	**Routing overhead**	**Throughput**	**Time**	**Delay**	**Energy**	**PDR**	**Routing overhead**	**Throughput**
Simple	0	0	0	0	0	0	0	0	0	0	0	0
	2	1054.99	23.52	0.6076	12	27.74	2	0	3.62	0	0	0
	4	1069.04	27.26	0.5341	3.61	29.35	4	8.8	12.77	0.6429	0.31	104.13
	6	1073.08	30.99	0.5267	4.452	28.22	6	9.79	13.01	0.6429	0.374	146.56
	8	1042.71	31.12	0.5539	5.96	24.77	8	9.67	13.19	0.6641	0.494	130.66
	10	1021	31.24	0.5725	7.516	22.59	10	9.93	13.45	0.6622	0.491	146.69
False Data Injection Data	0	0	0	0	0	0	0	0	0	0	0	0
	2	628.85	49.12	0.0317	1.895	151.02	2	0	3.62	0	0	0
	4	693.32	74.88	0.0109	4.526	194.14	4	8.87	12.76	0.7193	0.27	110.48
	6	1297.16	84.44	0.0099	4.614	184.96	6	11.66	13.03	0.6	0.338	151.99
	8	1912.04	86.79	0.0144	2.315	162.48	8	12.53	13.29	0.6263	0.518	140.2
	10	1988.42	87.34	0.0128	2.137	144.43	10	13.25	13.6	0.629	0.501	164.48
Session Attack	0	0	0	0	0	0	0	0	0	0	0	0
	2	108.16	56.3	0.0019	39	220.49	2	0	3.62	0	0	0
	4	1899.9	65.89	0.0058	12.15	183.81	4	8.37	12.76	0.7273	0.261	111.23
	6	1905.94	70.06	0.0038	35.19	248.32	6	11.11	13.04	0.6135	0.346	152.47
	8	2040.79	70.59	0.0032	34.79	251.97	8	12.18	13.29	0.636	0.52	141.08
	10	1666.79	72.95	0.0069	13.17	235.13	10	12.81	13.6	0.6341	0.521	162.18
Wormhole Attack	0	0	0	0	0	0	0	0	0	0	0	0
	2	381.82	47.27	0.0044	40.73	373.07	2	0	3.62	0	0	0
	4	1888.16	55.05	0.0093	10.43	308.14	4	8.43	12.77	0.6719	0.274	112.71

	6	2335.74	64.63	0.0087	7.1	240.67	6	10.26	13.1 0	0.6274	0.485	148.82
	8	2220.6	65.22	0.0095	4.133	199.64	8	10.07	13.33	0.6526	0.602	137.79
	10	1934.6	65.79	0.0105	2.72	181.24	10	11.8	13.56	0.6537	0.518	153.35



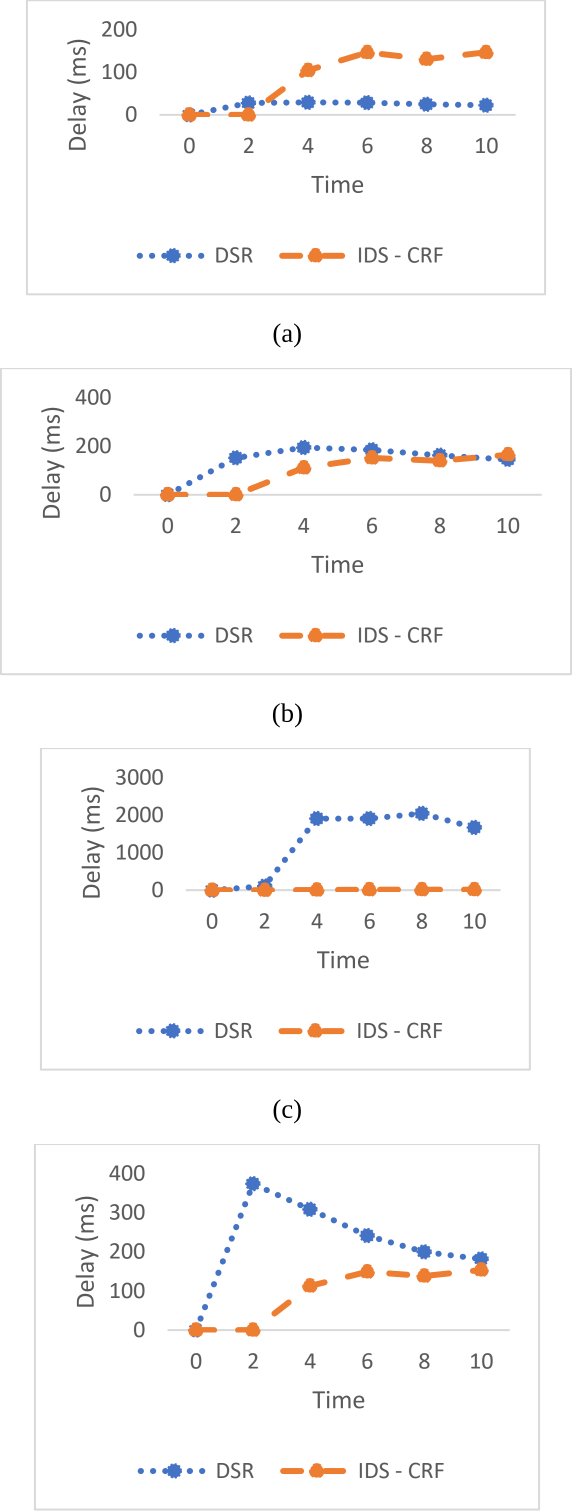
(a)

(b)

(c)

(d)

Fig. 4: Comparison of Delay (a)Simple (b) False Data Injection (c)Session Attack (d) Wormhole attack



(a)

(b)

(c)

(d)

Fig. 5: Comparison of Throughput (a)Simple (b) False Data Injection (c)Session Attack (d) Wormhole attack

From the above figure 4 and 5 it is evident that the performance of proposed secured version of IDS - CRF, is better when compared to the conventional DSR protocol in MANETs. a secure routing protocol called IDS - CRFfor MANET to protect the network from vulnerabilities and attacks. It is a security protocol with digital signature and DYDOG mechanism and integrated with two fish algorithms. Digital signature algorithm for receiving message authentication. Digital signature technology is used in two schemes, namely digital signature with message recovery function and digital signature with appendix. Whereas DYDOG is intrusion detection mechanism used to detect nodes that have been attacked or vulnerable. In this work, as an encryption technology, a 128-bit key length block cipher encryption algorithm called two fish algorithm is implemented. Therefore, each node carries a key. The digital signature is generated and encrypted with support of the two-phishing algorithm, which provides effective security for the network.

5. Conclusion

MANET security is an important parameter for secure data transmission over the network. This paper presented a Conventional Random filed-based IDS for secure data transmission. The proposed model uses the hashing function for the estimation of the variables in the network. The proposed model uses the discriminative CRF model for the generation of the security key in the MANET environment. The analysis of the results demonstrated that the proposed IDS – CRF model achieves the ~4% reduction in the delay and ~2% reduction in the routing overhead. Similarly, the proposed IDS – CRF model achieves the ~4% reduced energy consumption. In terms of the Packet delivery ratio and throughput the proposed IDS – CRF model achieves the ~4% - ~6% improved performance than the DSR protocol.

References

[1] Rathish, C. R., Karpagavadivu, K., Sindhuja, P., & Kousalya, A. (2021). A Hybrid Efficient Distributed Clustering Algorithm Based Intrusion Detection System to Enhance Security in MANET. *Information Technology and Control*, *50*(1), 45-54.

[2] Bandecchi, S., & Dascalu, N. (2021). Intrusion Detection Scheme in Secure Zone Based System. *Journal of Computing and Natural Science*, 19-25.

[3] Chawla, K., Gill, J., & Singh, M. (2021). Comprehensive Survey of IDS Techniques in Mobile Ad Hoc Network (MANET). *Soft Computing for Intelligent Systems*, 435-449.

[4] Gandage, S. C. (2021). AN EFFICIENT REVIEW OF IDS IN MANET USING PSO. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(12), 4873-4879.

[5] Khalifa, M. M., Ucan, O. N., & Alheeti, K. M. A. (2021, December). New Intrusion Detection System to Protect MANET Networks Employing Machine Learning Techniques. In *2021 International Conference of Modern Trends in Information and Communication Technology Industry (MTICTI)* (pp. 1-6). IEEE.

[6] Chawhan, M. D., Karmarkar, K., Almelkar, G., Borkar, D., Kulat, K. D., & Neole, B. (2022, April). Identification and prevention of Gray hole attack using IDS mechanism in MANET. In *2022 10th International Conference on Emerging Trends in Engineering and Technology-Signal and Information Processing (ICETET-SIP-22)* (pp. 1-6). IEEE.

[7] Gao, X., Du, W., Liu, W., Wu, R., & Zhan, F. (2020, December). A Lightweight and Efficient Physical Layer Key Generation Mechanism for MANETs. In *2020 IEEE 6th International Conference on Computer and Communications (ICCC)* (pp. 1010-1015). IEEE.

[8] Brindha, V., Karthikeyan, T., & Manimegalai, P. (2019). Fuzzy enhanced secure multicast routing for improving authentication in MANET. *Cluster computing*, *22*(4), 9615-9623.

[9] MOHINDRA, A. R., & GANDHI, C. (2021). A secure cryptography based clustering mechanism for improving the data transmission in MANET. *Walailak Journal of Science and Technology (WJST)*, *18*(6), 8987-18.

[10] Kaur, I., & Rao, A. L. N. (2013). Adaptive group key management in mobile ad-hoc networks (MANETs). *International Journal of Computer Applications*, *70*(11).

[11] Kumar, A., & Aggarwal, A. (2012, February). Performance analysis of MANET using elliptic curve cryptosystem. In *2012 14th International Conference on Advanced Communication Technology (ICACT)* (pp. 201-206). IEEE.

[12] MOHINDRA, A. R., & GANDHI, C. (2021). A secure cryptography based clustering mechanism for improving the data transmission in MANET. *Walailak Journal of Science and Technology (WJST)*, *18*(6), 8987-18.

[13] Wilson, A. J., & Radhamani, A. S. (2022). Real time flood disaster monitoring based on energy efficient ensemble clustering mechanism in wireless sensor network. *Software: Practice and Experience*, *52*(1), 254-276.

[14] Asaamoning, G., Mendes, P., & Magaia, N. (2021). A Dynamic Clustering Mechanism With Load-Balancing for Flying Ad Hoc Networks. *IEEE Access*, *9*, 158574-158586.

[15] Huang, C. M., Dao, D. T., & Mai, C. M. (2017, January). Location-Based Service (LBS) data sharing using the k-member-limited clustering mechanism over the 4G and Wi Fi hybrid wireless mobile networks. In *2017 International Conference on Information Networking (ICOIN)* (pp. 526-531). IEEE.

[16] Anil, G. N. (2021, April). Multi-level Trust Modelling to Resist Impact of Routing Attacks on Reliable Data/Communication Transactions in MANET-IoT Ecosystem. In *Computer Science On-line Conference* (pp. 196-205). Springer, Cham.