

# Performance Analysis of MANET under Rushing Attack



Shukla Mondal, Khondekar Lutful Hassan

**Abstract:** In this article performance analysis of MANET under rushing attack has been performed. It is mainly focused on the analysis of the effect of Rushing attack in MANET. Ad-hoc On-Demand Distance Vector (AODV) routing protocol is considered as the routing protocol of MANET. This paper will analyze the various results that how the attackers affect the performance of the routing protocol in the MANET. Network Simulator NS2 (2.35) is taken as simulation tools for simulation purpose. Various node densities are considered as simulation parameters, which are used for analysis of AODV protocol under Rushing Attack. Analysis of performance is based on Control Overheads, Normalized Routing Overheads, Delay and Throughput.

**Index Terms:** Rushing attack, MANET, AODV, Security, Routing Protocols, Byzantine Attack, Jellyfish Attack.

## I. INTRODUCTION

A MANET is defined as a self-organized collection of mobile nodes. Every node in MANET communicates themselves via wireless-links. It has neither any specified infrastructure nor any consolidated admin. In this network, the destination receives the packet and a routing protocol finds route by forwarding packets through the in between nodes towards it. A wireless-network is more adaptive than the wired one, but it has lot of security issues that makes it very unsafe. In case of MANET, networks have more security threat than wired networks because of the following reasons

First, it is Open Medium that means eavesdropping is very much easier than wired networks. Secondly, the Network topology changes dynamically, that's why any node comes and goes from the network, so any malicious nodes can join in the network without being detected. And it Lacks the Resources, it invokes the problem of limited security.

Just like any other networks, MANET has also some basic security goals. Mostly, Authentication or Authorization i.e. verification and identification of source information; Availability i.e. the ability of the networks that provides required service requests; Integrity i.e. data is not altered by any other person or environment which have no required

permission.

## II. LITERATURE REVIEW

Researchers have done many works to exploit the security of MANET. Few attacks occur in different layers. Repudiation occurs in Application Layer, TCP/UDP SYN flood and Session hijacking occurs in Transport Layer. Black hole attack, Worm hole attack, Rushing attack occurs in Network Layer. Monitoring and Traffic analysis occurs in Data link Layer. Eavesdropping, active interference occurs in Physical Layer. Some of the attacks occur in multiple layers [1]. These types of attacks are Denial of Service (DoS), SYN Flooding, Black hole attack, Wormhole attack, Repudiation etc. In Denial of Service (DoS) attack [2], attacker tries to prevent authorized users to access services given by the network. In SYN Flooding attack, it spoofs the return address of SYN packets by sending a huge amount of SYN by a malicious node to the victim node [3]. For Black hole attack [4], in a flooding-based protocol, an attacker listens to the request for the routers. It creates a reply consisting of extremely short route when it receives a route-request to the destination node. Then it enters that path and it does anything with all the packets that are being passed between them. In Wormhole attack [5], the affecting node gets the packet at some location in the network and re-route them to some other location and resent in the network. This re-route location is mentioned as wormhole. In case of Rushing Attack [6], it occurs during route discovery process On-Demand protocols like AODV, DSR etc. uses duplicate suppression can be affected by this attack. The attacker quickly forwards the route discovery packets by using the duplicate suppression technique and it gains access to the forwarding group. It can act as an effective Denial of Service (DoS) attack against all currently proposed routing on-demand protocols. The Repudiation refers to the denial node or the node which is attempting denial in the network [7]. Some Attacks can also be categorized as active attack and passive attack. In the Active attack, the data that are being exchanged, are tried to corrupt in this attack. But in the Passive attack, it does not actually disrupt any operation in the network. E.g. Snooping is the access to the unauthorized data.

## III. METHODOLOGY

Rushing attacks can be implemented with two methods. In this paper, Rushing attack is implemented by Byzantine attack and Jellyfish attack as the Rushing attack.

Manuscript published on November 30, 2019.

\* Correspondence Author

Shukla Mondal\*, Department of Computer Science and Engineering, Aliah University, Kolkata, India.

Khondekar Lutful Hassan, Department of Computer Science and Engineering, Aliah University, Kolkata, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

## Performance Analysis of MANET under Rushing Attack

The Byzantine attack can be done by dropping all packets or selectively; and done by modifying packets. In this paper, we have considered only dropping packets.

The Jellyfish attack can be done by two ways either by delaying packets or re-ordering packets. In this paper, we have considered only delaying packets.

### A. Pseudocode to Configure NS2 for Rushing Attacks

The following step by step procedure will show how it is implemented in NS2:

- Step 1: Define Rushing attackers in the header file (aodv.h):  

```
nsaddr_t malicious;
```
- Step 2: Declare a static integer variable *tm* in aodv source file (aodv.cc) and initialize it to 0.
- Step 3: Initialize Rushing attackers in AODV source code inside the AODV::command function  

```
if(strncasecmp(argv[1], "rushingattack", 13) == 0) {
    malicious= 10000;
    return TCL_OK;
}
```
- Step 4: Set *malicious=9999* in the function AODV::AODV (nsaddr\_t id).
- Step 5: Rushing attackers broadcast route request as follows:  

```
if(malicious==10000)
    increment hop count.
if(malicious==10000)
    forward aodv route entry without DELAY
else
    forward aodv route entry with DELAY
```
- Step 6: In forward packet definition in the aodv source file  

```
if ((channel payload type == payload type of AODV) && (malicious! =10000))
    Jitter the sending of AODV broadcast packets by 10ms
else
    No jitter i.e. no variation in the delay of received packets.
```
- Step 7: //only dropping packets is considered in Byzantine attack  

```
if ((channel payload type == payload type of AODV) && (malicious! =10000))
    if(tm < CURRENT_TIME)
        increment tm and drop the packets due to no route to destination.
// In Jellyfish attack, only delaying packets is considered
else
    forward route packet where delay of 1.0 is varied.
```
- Step 8: End.

### B. Performance Evaluation Metrics

For performance analysis of the network under MANET, it

is taken five different parameters that are:

- 1) *Packet Delivery Ratio (PDR)*: It is the percentage in which the no. of packets is received by the receiving node divided by the no. of total packets sent by the sender node.
- 2) *Control Overhead*: The overhead of maintaining routing information about the available path in the network.
- 3) *Normalized Routing Overheads*: It is defined as the number of routing packets transmitted per data packet.
- 4) *Delay*: A packet requires some unit time interval to transmit from source to destination.
- 5) *Throughput*: The number of packets is received successfully per second through the communication medium.

In this paper, to analyze the performance of the network it is taken that the 20% of the nodes as the Rushing attackers and compared with the 0% or no attackers in the network and Affected nodes are positioned anywhere in the network randomly.

## IV. SIMULATION PARAMETER SETUP

For the simulation purpose Network Simulator 2 (NS2.35) is taken as simulation tool. It is taken two types of parameters for simulations. One is fixed parameters and another is variable parameters. Fixed parameters are those parameters which are fixed during all the simulation and variable parameters are those parameters which are changed for every simulation for analysis purpose. Table I describes the list of fixed parameters with their values.

**Table I List of fixed parameters with their values which are used during simulation**

Parameters	Values
MAC type	Mac/802_11
Interface queue	DropTail/PriQueue
Link layer type	LL
Antenna model	OmmiAntenna
Max packet in	50
Routing protocol	AODV
Simulation time (stop)	200
Channel type	Wireless Channel
Radio-propagation model	TwoRayGround
Network interface type	Phy/WirelessPhy

The node density is considered as variable parameters in every simulation for analysis purpose. For this simulation, the nodes density is categorized into two categories. One is lower node density and another is higher node density. In lower node density, node number of 20, 25, 30, 35, 40, 45, 50 and 60 is considered. And in the higher node density node number of 80, 100, 120, 140, 200, 300 and 400 are taken.

For determination of the effect of the rushing attack, two types of nodes are considered here. One is malicious node that means those nodes which is affected by rushing attackers. Here 20% nodes are taken as malicious nodes. Affected nodes are positioned anywhere in the network randomly. Another type of nodes is 0% attack that means no attack is occurred in the network.

It is taken three scenarios for the topographical dimension to determine the effect of rushing attack in detail. The scenarios are 500X500, 1000X1000 and 2400X2400. The detail result is described in the section V.

V. RESULT ANALYSIS

Now, it is discussed about the various results from the simulation with the Rushing attacks that is implemented. It is analyzed the performance of the network under the five-various performance parameter one by one that is mentioned earlier. All the mentioned parameters are analyzed in three scenarios of the topographical dimension. The scenarios are explained in two cases – lower node density and higher node density that has already mentioned earlier.

A. Analysis of Packet Delivery Ratio (PDR)

PDR is the rate of receive packet by the receiving nodes. It is measured by the percentage in which the no. of packets is received by the receiving node divided by the no. of total packets sent by the sender node.

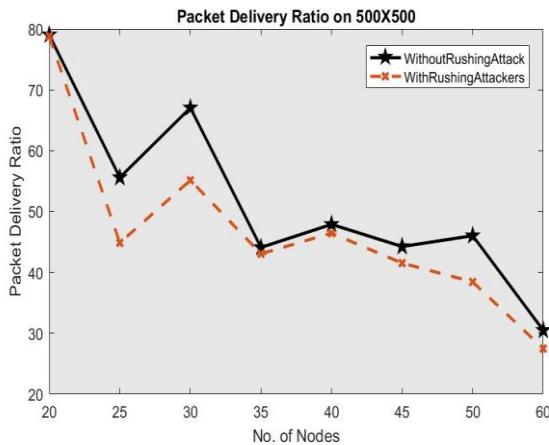


Figure 1 PDR with lower load density on 500X500

In the Fig. 1 and Fig. 2, it is seen that packet delivery ratio is always less with the rushing attackers in both lower node density and higher node density in scenario 500X500.

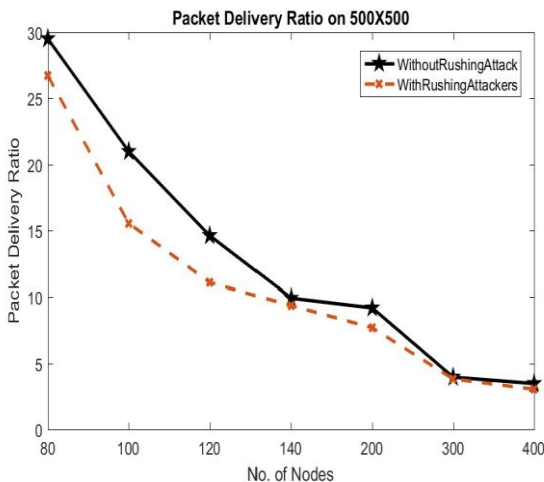


Figure 2 PDR with higher node density on 500X500

Few cases of the simulation it is seen that packet delivery ration (PDR) of both malicious and non-malicious simulation is same. The cause of such type of situation may be occurred due to some other parameters like, high node speed, dynamic node deployment, higher node density etc. Most of the cases it is seen that the rushing attack affect the packet delivery ratio of entire network. Packet delivery ratio of network containing malicious node is less than the network which is not containing any malicious node.

B. Analysis of Control Overhead

Control overhead is defined as the overhead of maintaining routing information about the available path in the network. Control overhead of the networks in case of three scenarios mentioned is seen in the Fig. 3 and Fig. 4 subsequently. The control overhead is supposed to be more of the network with the Rushing attack than the network without the rushing attack, but sometimes it is violating. This type of cases occurred due to some external factors like high node speed, dynamic node deployment, higher node density, congestion, collision etc.

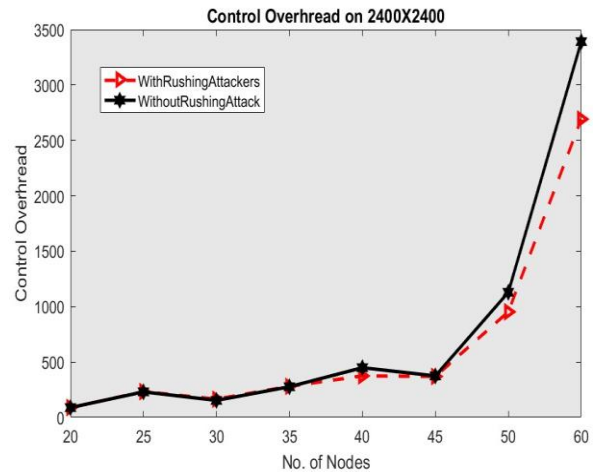


Figure 3 Control overhead with lower node density on 2400X2400

Comparison of the control overhead of the network with rushing attack and the network without rushing attack in scenario 2400X2400 is shown in the Fig. 3 and Fig. 4.

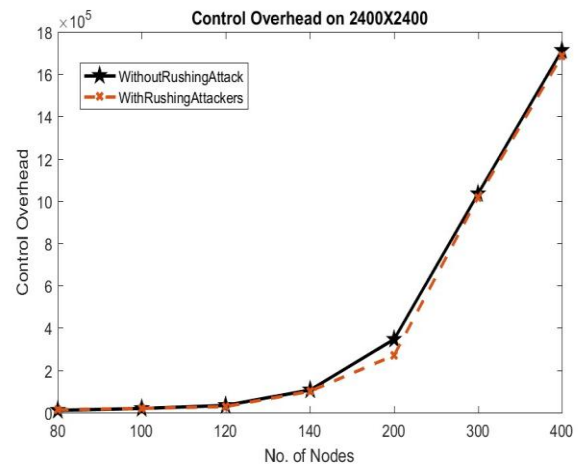


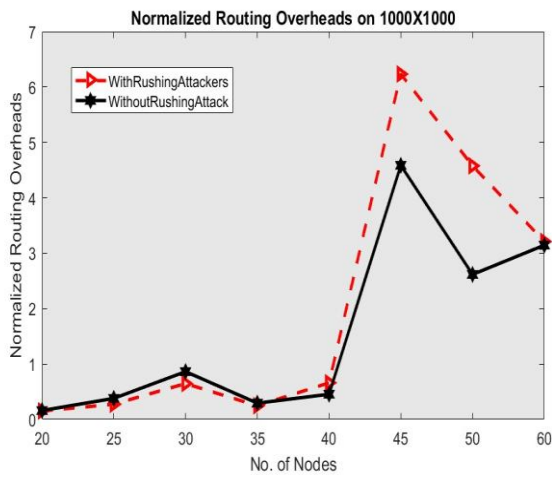
Figure 4 Control overhead with higher node density on 2400X2400

It is seen that control overhead of the network belonging the rushing attack does not cross the derivation with the control overhead without attacker nodes. In the node number of 50 and 60 it is seen that control overhead of the rushing attack is higher than the network belongs no rushing attack.

C. Analysis of Normalized Routing Overhead

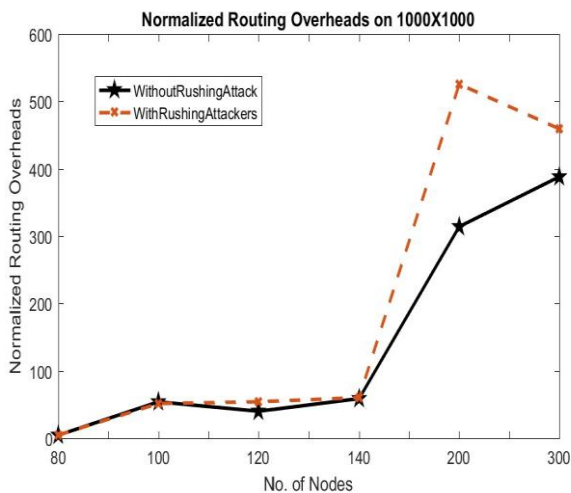
Comparison of the normalized routing overheads of the network with rushing attack and the network without rushing attack in scenario 1000X1000 is shown in the Fig. 5 and Fig. 6 respectively.

## Performance Analysis of MANET under Rushing Attack



**Figure 5 Normalized Routing Overheads with lower node density on 1000X1000**

It is seen that in lower node density when the node density is 30 and 40 the normalized routing overhead is less of the network belongs to the rushing attack than the network which does not belongs the rushing attack.

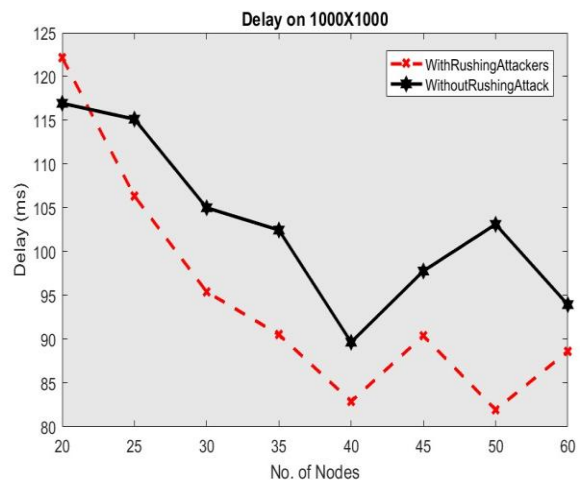


**Figure 6 Normalized Routing Overheads with higher node density on 1000X1000**

It is happened due to some other parameters like, high node speed, dynamic node deployment, higher node density, congestion, collision etc. But in other cases, it does not cross the derivation with the other.

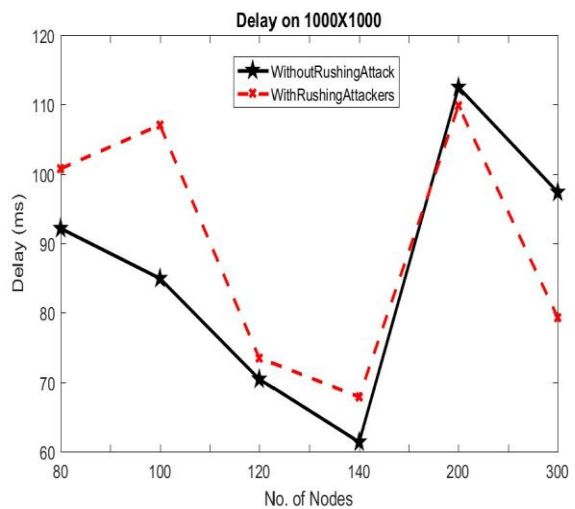
### D. Analysis of Delay

Delay is defined as a packet requires some unit time interval to transmit from source to destination. Comparison of the end to end delay of the network with rushing attack and the network without rushing attack in scenario 1000X1000 is shown in the Fig. 7 and Fig. 8 respectively. It is seen that delay of the network which belonging the rushing attack is lower than the network not belonging any rushing attack in the lower node density., but in higher node density most of the cases it is much higher of the network with the rushing attack than the network without rushing attack.



**Figure 7 Delay with lower node density on 1000X1000**

In some cases, the network belongs the rushing attack has got lower normalized delay than the network belongs no rushing attack .it is happened due to some other parameters like, high node speed, dynamic node deployment, higher node density, congestion, collision etc.



**Figure 8 Delay with higher node density on 1000X1000**

### E. Analysis of Throughput

Throughput is defined as the number of packets is received successfully per second through the communication medium. Comparison of the throughput of the network with rushing attack and the network without rushing attack in scenario 500X500 is shown in the Fig. 9 and Fig. 10 respectively. It is seen that throughput of the network which belonging the rushing attack is always less than the throughput of the network not belonging any rushing attack. The cause of the type of result is that the rushing attack always drops the data packet in the malicious node. For that reason, throughput of the network with rushing attack is always less than the network without any attack.

In the Fig. 9 and Fig. 10, it is seen that the throughput is significantly less of the network belonging the rushing attack in both lower node density and higher node density in the scenario 500X500.

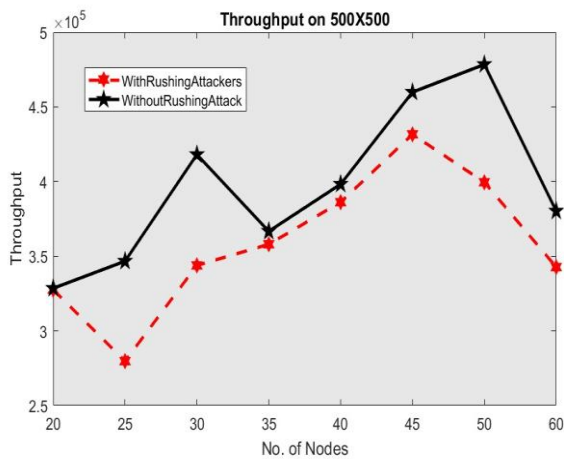


Figure 9 Throughput with lower node density on 500X500

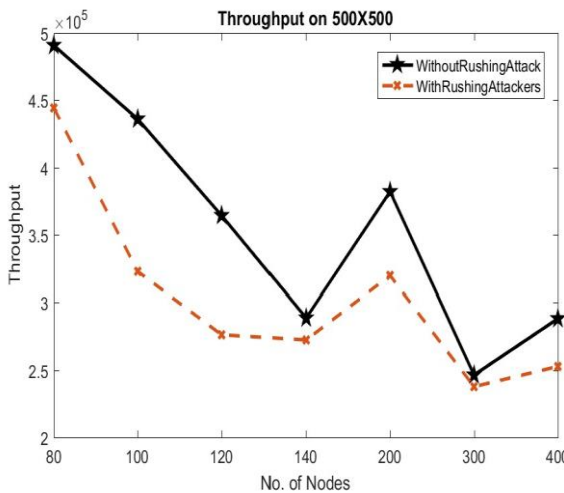


Figure 10 Throughput with higher node density on 500X500

## VI. CONCLUSION

It is seen from the above analysis that Rushing attack affects the performance significantly in the network. All the five parameters that is analyzed in the network with and without the attacker nodes, clearly shows that Rushing attack is a big security threat for the network. In this paper, it is shown the rushing attack in a network of multiple senders, multiple receivers and attacker node in anywhere in the network in case of three different topographical area. In all the cases, malicious nodes affect the network and degrade its performance. Some of the performance parameters it is discussed like throughput and packet delivery ratio, they are always affected by the rushing attack significantly. In all other cases too, it degrades the performance significantly. In future work, it can be analyzed other protocols with other attacks in lower node density as well as in higher node density too.

## REFERENCES

1. Gao Liu, Zheng Yan, Witold Pedrycz, "Data collection for attack detection and security measurement in Mobile Ad Hoc Networks: A survey", *Journal of Network and Computer Applications*, Vol. 105, pp 105-122, 2018.
2. Khan M.S., Jadoon Q.K., Khan M.I., "A Comparative Performance Analysis of MANET Routing Protocols under Security Attacks" *Mobile and Wireless Technology 2015. Lecture Notes in Electrical Engineering*, Springer, Berlin, Heidelberg, vol 310, 2015.

3. Hoang Lan Nguyen, Uyen Trang Nguyen, "A study of different types of attacks on multicast in mobile ad hoc networks", *Ad Hoc Networks*, Volume 6, Issue 1, Pages 32-46, January 2008.
4. Pandi Selvam Raman, "A Study of Black Hole Attack and its Recent Prevention Techniques in MANET", *International Journal of Computer Applications (0975 – 8887)*, Vol. 162 – No 8, March 2017.
5. Divya Sai Keerthi Tiruvakadu, Venkataram Pallapa, "Confirmation of wormhole attack in MANETs using honeypot", *Computers & Security*, Volume 76, pp 32-49, 2018.
6. W. Junaid, A. Iqbal, "Prevention of Multiple Rushing Attacks in Mobile Ad Hoc Network Using AODV Routing Protocol", *Sci.Int.(Lahore)*, 30(1), 173-177, 2018.
7. H. Moudni, M. Er-Rouidi, H. Mouncif and B. El Hadadi, "Attacks against AODV Routing Protocol in Mobile Ad-Hoc Networks", 2016 13th International Conference on Computer Graphics, Imaging and Visualization (CGiV), Beni Mellal, 2016, pp. 385-389.
8. L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks", *IEEE Network Magazine*, Volume. 13, no. 6, Pages 24-30, December 1999.
9. P. Goyal, S. Batra, A. Singh, "A Literature Review of Security Attack in Mobile Ad-Hoc Network", *International Journal of Computer Science and Information Security (IJCSIS)*, Vol. 4, No. 1 & 2, 2009.
10. D. Bruschi, and E. Rosti, "Secure Multicast in Wireless Networks of Mobile Hosts", *Protocols and Issues, Mobile Networks and Applications*, Volume 7, 2002, pp 503 - 511.
11. S. Corson, J. Macker, "Mobile ad hoc Networking (MANET)", *Routing Protocol Performance Issues and Evaluation Considerations*, RFC 2501, January 1999.
12. F. Abdel-Fattah, K. A. Farhan, F. H. Al-Tarawneh and F. AlTamimi, "Security Challenges and Attacks in Dynamic Mobile Ad Hoc Networks MANETs," 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), Amman, Jordan, 2019, pp. 28-33.

## AUTHORS PROFILE



**Shukla Mondal** received his Bachelor degree in Computer Application from Maulana Abul Kalam Azad University of Technology (formerly known as WBUT), India, in 2015. He received his Master degree in Computer Application from Aliah University, India in 2018. He is currently pursuing M.Tech degree in

Computer Science and Engineering in the Department of Computer Science and Engineering, Aliah University, India. Since 2018, his research interests focus on MANET security.



**Khondekar Lutful Hassan** is currently working as Assistant Professor in Department of Computer Science and Engineering, Aliah University, Kolkata, India. He holds a Bachelor degree in Computer Science and Engineering from Govt College of Engineering and Ceramic Technology, and M.Tech degree from University of Calcutta, Calcutta, India in the year of 2010 and 2012 respectively. His research interests include Mobile Ad-hoc Network, Network Security etc.