Recent Research in Science and Technology 2021, 13: 1-5
doi: 10.25081/rrst.2021.13.6848
http://updatepublishing.com/journal/index.php/rrst

Research Article

ISSN: 2076-5061

Smart detection and prevention procedure for DoS attack in MANET

A. S. M. Muntaheen[1], Milton Chandro Bhowmick[1], Md. Raqibul Hasan Rumman[1], Nayeem Al-Tamzid Bhuiyan[2], Md. Taslim Mahmud Bhuyain[3], Md. Rakibul Islam[3], Md. Babar Ali Bhuyan[3], Md Sahadat Hossain Sagor[4], Md. Imdadul Hoque[5], Md. Majharul Islam[6]*, Md. Mahmudul Hasan[2]

[1]Department of Computer Science and Engineering, Military Institute of Science and Technology, Dhaka - 1216, Bangladesh, [2]Department of Electrical and Computer Engineering, North South University, Dhaka - 1229, Bangladesh, [3]Department of Information and Communication Engineering, Noakhali Science and Technology University, Noakhali – 3814, Bangladesh, [4]Department of Information Technologies, Czech University of Life Science, Kamýcká 129, 16521 Prague, Czech Republic, [5]Department of Communication and Information Technology, University of Bremen, 28359 Bremen, Germany, [6]Department of Information and Communication Technology, Friedrich Alexander University, 91054 Erlangen, Germany

ABSTRACT

A self-organized wireless communication short-lived network containing collection of mobile nodes is mobile ad hoc network (MANET). The mobile nodes communicate with each other by wireless radio links without the use of any pre-established fixed communication network infrastructure or centralized administration, such as base stations or access points, and with no human intervention. In addition, this network has potential applications in conference, disaster relief, and battlefield scenario, and have received important attention in current years. There is some security concern that increases fear of attacks on the mobile ad-hoc network. The mobility of the NODE in a MANET poses many security problems and vulnerable to different types of security attacks than conventional wired and wireless networks. The causes of these issues are due to their open medium, dynamic network topology, absence of central administration, distributed cooperation, constrained capability, and lack of clear line of defense. Without proper security, mobile hosts are easily captured, compromised, and attacked by malicious nodes. Malicious nodes behavior may deliberately disrupt the network so that the whole network will be suffering from packet losses. One of the major concerns in mobile ad-hoc networks is a traffic DoS attack in which the traffic is choked by the malicious node which denied network services for the user. Mobile ad-hoc networks must have a safe path for transmission and correspondence which is a serious testing and indispensable issue. So as to provide secure communication and transmission, the scientist worked explicitly on the security issues in versatile impromptu organizations and many secure directing conventions and security measures within the networks were proposed. The goal of the work is to study DoS attacks and how it can be detected in the network. Existing methodologies for finding a malicious node that causes traffic jamming is based on node's retains value. The proposed approach finds a malicious node using reliability value determined by the broadcast reliability packet (RL Packet). In this approach at the initial level, every node has zero reliability value, specific time slice, and transmission starts with a packet termed as reliability packet, node who responded properly in specific time, increases its reliability value and those nodes who do not respond in a specific time decreases their reliability value and if it goes to less than zero then announced that it's a malicious node. Reliability approach makes service availability and retransmission time.

KEYWORDS: MANET, Security Attacks, DoS, DDoS, Intruder, Tapping

Received: October 02, 2020
Accepted: January 22, 2021
Published: January 29, 2021

***Corresponding Author:**
Md. Majharul Islam
E-mail: majharulislam.ice@gmail.com

INTRODUCTION

By dealing with self-maintenance and self-configuration properties or behavioral properties, mobile ad hoc networks got outstanding success as well as tremendous attention in the field of communication. The mobile or portable devices are free to move at any rate or direction and are part of the network only when they are within range. Mobile ad hoc networks (MANET) are interchangeably referred to as Ad hoc or ad-hoc networks. MANET is a set of devices or nodes that transmit data across a wireless communication medium mostly based on radio frequency without any existing fixed infrastructure or centralized control. There will be no middle control or infrastructure of network for a MANET to be set up, therefore making its deployment immediate and inexpensive.

Since they are often used in critical applications where data and communications integrity is important therefore securing MANETs is an important part of deploying and utilizing them. Availability of network services, confidentiality, and integrity of the data can be achieved by assuring that security issues have been met. However, MANET often has issues with several security attacks because of its features are open medium, changing its topology dynamically, cooperative algorithms, lack of central monitoring and management, and no clear defense mechanism. The above-discussed factors have changed the battlefield situation for the MANET against security threats.

Mobile ad hoc networks have several loop-false due to their infrastructure-less environment structure. These loop-false are the gateway to make opportunity for attackers to influence the smoothness and steadiness of network operations. Attacker or unauthorized person can attempt different attacks by identifying loop-false in the network, which is violating security policies of the network. One of them is a DoS attack to infer such policies (below).

- Availability
- Confidentiality
- Authenticity

Moreover, attacks influence different network resources also those are precious for running network process. Some of them characterized underneath:

- Battery power
- Routing overhead
- Lifetime
- Packets delay
- Throughput

Several mechanisms and protocols are advised on individual black hole attacks. Therefore, it is required to do more work on the DoS attacks, which were approached by researchers. The existing advised approaches have certain problems and glitches. Firstly, node sent data packet to determine the value of reliability levels of nodes in the network. When nodes play the role of a black hole in a certain group then it does not send acknowledgement of data packet because of these watch data packets only. So, in this scenario data packet of the sender read by black hole node. Secondly, it is too difficult to detect node as black hole when its reliability level value zero initially when the network is deployed. Thus, we required an approach to prevent data packet and perfect detection of DoS attack nodes in the network.

RELATED WORK

Due to various factors including lack of infrastructure, absence of already established trust relationship between the different nodes, and dynamic topology, the routing protocols are vulnerable to various attacks. Major vulnerabilities that have been so far researched are mostly these types which include selfishness, dynamic nature, and severe resource restriction, and also open network medium. A number of researches are done on security challenges and solutions in mobile ad hoc network: Schmidt and Trentin (2008) proposes that an effective MANET routing protocol must be equipped to deal with the dynamic and unpredictable topology changes associated with mobile nodes, whilst also being aware of the limited wireless bandwidth and device power considerations which may lead to reductions in transmission range or throughput. In the trade-model, each and every device has a tamper-resistant security module, public key infrastructure (PKI) to guarantee its validation, so it is used for account management. Two billing mechanisms were introduced that charge nodes as a function of number of hops messages have been traveled (Majumder *et al.*, 2011). A reputation-based scheme that discovers the effect of misbehavior on network performance was introduced. It uses a watchdog mechanism to rectify improper nodes and a path rater for selecting routes that do not choose misbehaving nodes (Giordano & Stojmenovic, 2004). Luo *et al.* (2009) introduced the main problem of detecting pulsing denial of service (PDoS) attacks which send a series of attack pulses to decrease transmission control protocol throughput. Lin *et al.* (2008) have presented a mechanism to observe the traffic pattern in order to alleviate DDoS. Yi *et al.* (2009) have proposed a new Denial of Service attack and its defense mechanism in ad-hoc networks. The new DoS attack, known as Ad-hoc Flooding Attack (AHFA), can result in denial of service (DoS) when used against on demand routing protocols for MANET. Paul *et al.* (2019) have presented Denial of Service (DoS) elimination technique which uses digital signatures to authenticate legitimate data and plunge packets that do not pass the validation.

PROBLEM DEFINITION

Mobile ad hoc networks are generally more vulnerable to physical security threats than fixed-cable networks. Portable or Dynamic nature characteristics sometimes become vulnerable point for attackers to disturb network systems or degrade network performance and lifetime (Gao *et al.*, 2019). Due to dynamic nature property of ad-hoc network several kinds of attack possible on networks which break security goals.

Black Hole Attack

In black hole attack, a malicious node uses its routing protocol in order to publicize itself for having the shortest route to the destination node. This aggressive node publicizes its availability of fresh routes regardless of checking its routing table. In this attack, attacker node always has the accessibility in replying to the route request. So, the node adapts the data packet and drop it. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from any actual node. Therefore, a malicious and fake route will be created. When this route has been set up, now it is depending on the node whether to drop the packet or to forward them to an unknown (Alsumayt *et al.*, 2018).

The method of how malicious node fits in and also how the data routes change, Figure 1 displays how the black hole problem

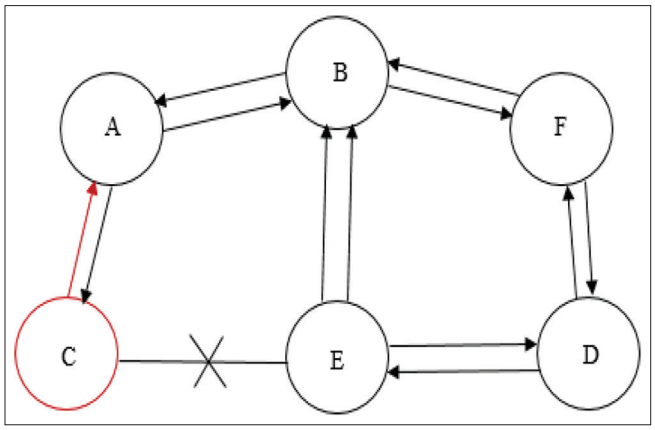

Figure 1: Black Hole Attack (Fazeldehkordi *et al.*, 2016)

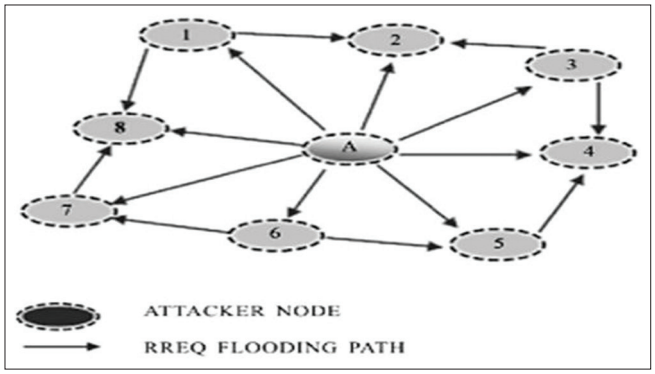

Figure 2: Gray Hole Attack (Dixit *et al.*, 2015)

appears. Here node "A" wants to communicate to node "D" and send data packets, thus the route discovery process initiates. Node "C" is a malicious node then it will claim that it has active route to the specified destination node as soon as it receives RREQ packets from node "A". It will then send RREP to node "A" before any other actual node. In this way, node "A" will assume that this is the active route so active route discovery is completed. After that node, "A" will ignore all other replies and start sending data packets to node "C". And finally, node "C" will drop all the data packets so they will be consumed or lost.

DoS and Flooding

DoS and flooding attacks are the most common attacks in MANET. Flooding attacks are of two types RREQ packet flooding and DATA flooding attacks. Flooding means a huge amount of RREQ packets or DATA packets are sent for the purpose of wastage of resources or consume more resources. In Denial-of-Service (DoS) attack, an attacker attempts that legitimate users are not able to access information or services. These packets increase unnecessary traffic in the network so that the congestion problem arises. The attacker acts as a malicious which sends packets flooding to discharge battery power of the genuine node. The most common and noticeable type of DoS attack occurs when an attacker floods a network with information and the server can only process a certain number of requests at a time, so if an attacker puts burden of RREQ packets on the server it cannot process the legitimate request.

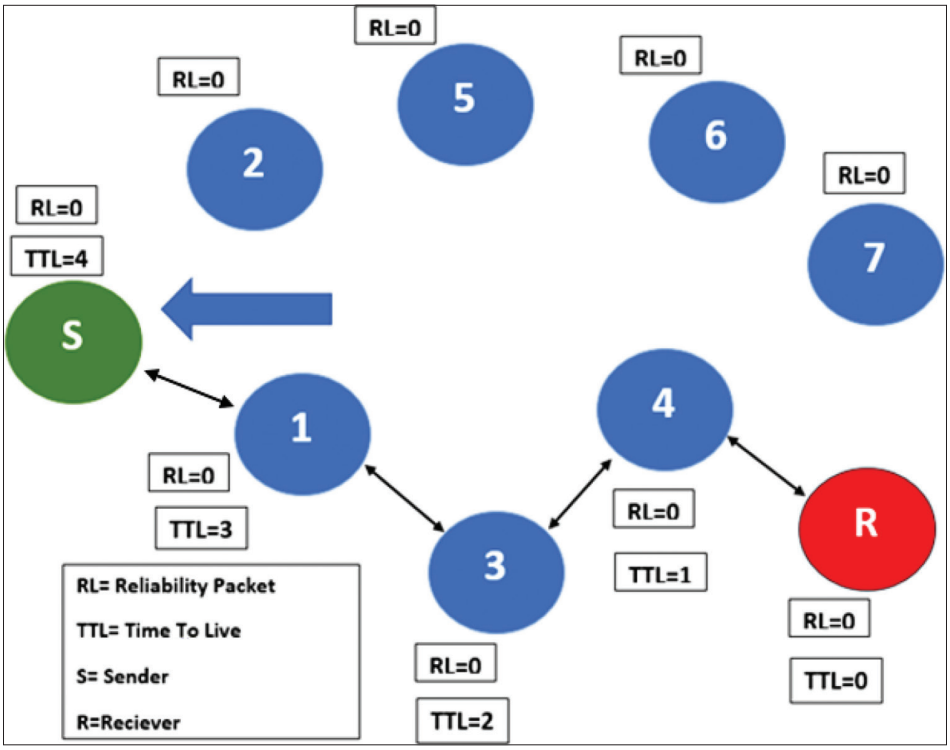

Figure 3: Data Transmission

Gray Hole Attack

A Gray-hole attack is similarly related to the two-attack black hole and worm-hole attack (Figure 2). In this attack nodes forward all packets to some nodes, but may drop packets coming from or ordained to specific nodes. This type of attack is more complicated compared to black hole attack. Problem Definition- Multi-Hop wireless network has several loop-false due to infrastructure-less environment. These loop-false makes opportunity for attackers to influence the smoothness of network operations. Attacker or unauthorized person can put different attacks by identifying loop-false in the network, which is violating security policies of the network. One of them is a DoS attack to infer such policies (below).

- Availability
- Confidentiality
- Authenticity

Additionally, attacks influence different network resources, also those are precious for running network process. Some of them are defined below:

- Battery power
- Lifetime
- Throughput
- Packets delay
- Routing overhead

For existing advised approach, several problems were detected. Firstly, node sent data packet to determine the value of reliability levels of nodes in the network. Secondly, it is too difficult to detect a node as malicious when its reliability level value zero initially when the network is deployed. Thus, we required new approaches to prevent data packet and perfect detection of malicious nodes in the network.

Proposed Mechanism

Mobile ad hoc networks have several drawbacks due to their infrastructure-less environment and usual approaches. These loop-false creates chances for attackers to influence the smoothness of network operations. Attacker can put different attacks by identifying drawbacks in the network, which is violating security policies of the network. Additionally, attacks influence different network resources also those are precious for running network process such as throughput, battery power, routing overhead, and end to end packet delay. Several mechanisms and protocols are advised on detection of DoS attacks but additional works should be introduced. To provide a solution for identified problem, a mechanism is proposed to prevent data packet loss occurs during the determining TTL value of nodes and detection of malicious attacks in the network. The mechanism proposed uses an additional packet named as reliability packet (RL packet) before of data packet to determine the TTL value of nodes. The RL value of node is incremented when it receives acknowledgement in specific time slice otherwise it is decremented when it does not receive acknowledgement in specific time slice. Each node has a routing table that contains path for every node. The node checks the RL value of nodes if it has extremely fluctuated or not normal, then node declared as malicious or compromised by DoS.

Proposed Algorithm

A. Algorithm

```
Algorithm RL_Mechanism(node,n)
{ Set RL v: =0;
    Set TS: =0;
    For i: =1 to n step i: =i+1 do
    node[i]:= RLV;
Send (node[i], node[j], RREQ);
node[i] wait for acknowledgement from node(j);

For TS: =0 to 2 step TS: =TS+1 do
    If (node[i]:Receive(node[j],RREP))
        RLv=RLv + 1;
    Else
        RLv=RLv -1;
    End
    if
Exit
}
If (node[i]==RLv>0)
    Send (node[i], node[j], DATA);
Else
    Declared (node [i+1], Malicious Node)
End

if

Exit

}
```

Operation

- Initially all nodes in the network have reliability packet and Time Slice (TS) zero.
- Source Node Send RREQ to its neighboring nodes and start Time Slice Timer. If the source node got a response in Specific Time Slice (in 3sec.) from neighbor node, then the responded node Reliability packet incremented by one (RLv=0+1) else it is decremented by one (RLv=0-1).
- And the process continues until the TTL value will become zero.
- Response include: RREP and RERR (Mapenduka, 2018)

CONCLUSION

Customary network needs a static infrastructure to set up, but MANET has a wide range of various approaches. Mobile ad hoc networks do not require a fixed infrastructure. It has the flexibility of a node that they can join a network or leave to a network at any time. The offered methodology tried to detect the malicious node in the network. Security of

the network is one of the essential features for its deployment (Mapenduka, 2018). Nodes disturb packet transmission and they try to receive transmitted data. In this paper, we have deeply engaged in detection of DoS attacks. It is the basic motivation of our work to define new approach to follow a different way to identify DoS attack by introduced an RL packet send at the beginning of communication when all nodes have RL value zero. Our Approached work is tracking response of nodes that means those nodes who reply to sender of packet in each time slice (TS) than grow its Reliability packet (RL) value by 1 but it can be in case questionable node that it may not answer to sender so if a sender does not get an acknowledgement from a receiver node in time slice than the sender decrement Reliability packet (RL) value of that node by 1. When a node reaches less than 0 it announces as a malicious node. Our methodology decreases the packet drop ratio and it reduces re-transmission time.

FUTURE WORK

Wireless Ad-Hoc networks are extensively used networks due to their flexible infrastructure. These networks are manifested in both external and internal attacks since there is no centralized security process. By this work, we try to find out the DoS attacks in MANET system and there are more possibilities to find such malicious nodes in the network. It provides a proper valid mechanism to decrease the possibility of obstacles from those ambiguous nodes. It becomes easier to transmit data freely. There is also certain area available in which researchers have to find the impact of the DoS attack in other MANET routing protocols such as DSR, TORA, and GRP along with AODV and OLSR protocols.

CONFLICTS OF INTEREST

The authors declare that they have no competing interests.

FUNDING

There is no funding to be disclosed.

REFERENCES

Alsumayt, A., Haggerty, J., & Lotfi, A. (2018). Evaluation of detection method to mitigate DoS attacks in MANETs. 1st International Conference on Computer Applications and Information Security, (pp. 1-5) Riyadh https://doi.org/10.1109/CAIS.2018.8441952

Dixit, S., Joshi K. K., & Joshi, N. (2015). A Review: Black Hole & Gray Hole Attack in MANET. *International Journal of Future Generation Communication and Networking*, 8(4), 287-294. http://dx.doi.org/10.14257/ijfgcn.2015.8.4.28

Fazeldehkordi, E., Amiri, I. S., Akanbi, O. A. (2016). A study of black hole attack solutions: On aodv routing protocol in manet. *Syngress* (pp. 7-57). https://doi.org/10.1016/B978-0-12-805367-6.00002-8

Gao, Y., Wu, H., Song, B., Jin, Y., Luo, X., & Zeng, X. (2019). A distributed network intrusion detection system for distributed denial of service attacks in vehicular ad hoc network. *IEEE Access, 7*, 154560-154571. https://doi.org/10.1109/ACCESS.2019.2948382

Giordano, S., & Stojmenovic, I. (2004). Position Based Routing Algorithms for Ad Hoc Networks: A Taxonomy. In X. Cheng, X. Huang & D. Z. Du (Eds.), Ad Hoc Wireless Networking. Network Theory and Applications. (pp. 103-136). Springer, Boston, MA. https://doi.org/10.1007/978-1-4613-0223-0_4

Lin, C. H., Liu, J. C., Huang, H. C., & Yang, T. C. (2008, April 2). Using adaptive bandwidth allocation approach to defend DDos attacks. International Conference on Multimedia and Ubiquitous Engineering (pp. 176-181). IEEE. https://doi.org/10.1109/MUE.2008.23

Luo, X., Chan, E. W. W., and Chang, R. K. C. (2009). Detecting pulsing denial-of-service attacks with nondeterministic attack intervals. *EURASIP Journal on Advances in Signal Processing, 2009*, 256821. https://doi.org/10.1155/2009/256821

Majumder, K., Ray, S., & Sarkar, S. K. (2011). Design and analysis of a multi-level location information based routing scheme for mobile ad hoc networks In X. Wang (Eds.), Mobile ad-hoc networks: Applications. IntechOpen (pp. 473-488). https://doi.org/10.5772/13053

Mapenduka, W. (2018). Methods for detecting attacks in *mobile/wireless ad-hoc networks: A Survey. International Journal of Scientific and Technology Research, 7*(7), 168-174.

Paul, S., Chitodiya, A., & Vishwakarma, D. (2019). Detection and Prevention Methodology for DoS Attack in Mobile ad-hoc Networks. *International Research Journal of Engineering and Technology, 6*(5), 6313-6317.

Schmidt, R, O., & Trentin, M. A. S. (2008). MANETs routing protocols evaluation in a scenario with high mobility MANET routing protocols performance and behavior," NOMS 2008 - 2008 IEEE Network Operations and Management Symposium, Salvador, Bahia, 2008, pp. 883-886. https://doi.org/10.1109/NOMS.2008.4575238

Yi, P., Zhou, Y-k., Wu, Y, & Liu N. (2009). Effects of denial of service attack in mobile ad hoc networks. *Journal of Shanghai Jiaotong University (Science), 14,* 580. https://doi.org/10.1007/s12204-009-0580-7