

## Preventive mechanism against DDoS attacks in MANET



Tariq Ahamad \*, Abdullah Aljumah

College of Computer Engineering &amp; Sciences, Prince Sattam Bin Abdulaziz University, Al-Kharj, Saudi Arabia

### ARTICLE INFO

#### Article history:

Received 30 January 2017

Received in revised form

8 March 2017

Accepted 17 April 2017

#### Keywords:

MANET

DDoS

Security

IDS

IPS

### ABSTRACT

A prevention technique is proposed in this article against DDoS attacks which consume the bandwidth in modern MANETS. Since these networks are wireless and self-configuring and doesn't need a pre-existing infrastructure and have a large unpredictable node movements, security becomes one of the most vital issue to be raised into the account. The proposed approach is based on the analysis and investigations of bandwidth attacks that mainly focus on DDoS that is truly a ruthless challenge and is difficult to detect, and decreases the performance of the network. DDoS includes a group of attacker nodes and targets the victim to prevent the legitimate users from accessing the network services and resources. Intrusion prevention system are the procedures that are treated as Add-ons' of the intrusion detection system to actively defend and prevent the intrusions, that are detected by the detection procedures of the IDS. The report that is generated by the IDS after analyzing the report of the forensic analysis is the base of the proposed procedure.

© 2017 The Authors. Published by IASE. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

### 1. Introduction

One of the major challenges faced by MANETs today is the security. As we all know traditional wired networks are relatively more secure than their wireless counterparts. Conventional infrastructure networks allows the traffic to travel through different routing devices like switches, gateways etc. which are often secured with a highly configured firewalls and many other security management techniques (Aljumah and Ahamad, 2016). So, these networks are well equipped against any type of intrusion or Denial of Service (DOS) attacks. On the other hand, the MANETs also known as peer-to-peer networks are wireless in nature, and are inherently vulnerable to different types of attacks (Aldaej and Ahamad, 2016).

The conventional protocols of wired networks are not suitable to implement in the ad-hoc environment, where the topology of the nodes changes frequently, the communication links between network nodes are wireless and there is no centralized control in the network (Xiang et al., 2011). So, it is necessary for each communicating node to incorporate some kind of security mechanism to prevent any kind of attacks.

### 2. Vulnerabilities in MANETs

Vulnerability is considered as imperfection in the security system. Any system is vulnerable if a user has unauthorized access to the data without proper identification (Ahmad and Aljumah, 2015). MANETs are more prone to such vulnerabilities due to their lack of central control, scarce resources, limited bandwidth, wireless medium of communication, node mobility, scalability etc. Wireless links are specifically vulnerable to spoofing, eavesdropping, replay, and many other attacks. It is evident from the literature that there is no clear line of protection in the network (Aad et al., 2008). The existing nodes in the network move freely in any direction and the new nodes join the network; some of the nodes maybe compromised by an adversary to perform some malicious behavior in the network (Nadeem and Howarth, 2009). Every contributing element in the ad-hoc networks is susceptible to internal as well as external threats. As, a result the MANETs require robust security scheme to ensure the network security.

### 3. Attacks in MANETs

There are mainly two types of attacks in MANETs; which are internal and external attacks. The internal attacks are far more dangerous than the external attacks. In the internal attacks the adversary tries to gain access of the network by compromising a node(s) credentials and acts as a legitimate node in the network (Alicherry et al.,

\* Corresponding Author.

Email Address: [tahanger@psau.edu.sa](mailto:tahanger@psau.edu.sa) (T. Ahamad)

<https://doi.org/10.21833/ijaas.2017.05.017>

2313-626X/© 2017 The Authors. Published by IASE.

This is an open access article under the CC BY-NC-ND license

(<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

2009). After gaining the access, the intruder can launch variety of attacks on the network. It can analyze the traffic between the nodes and can contribute in the network operation in a negative way. Whereas, the external attacks aims to create congestion, fake routing, and disturb the smooth functionality of the network (Ahamad and Aljumah, 2015). The network attacks are further classified into active and passive attacks. In active attacks the intruder participates actively in the network and launches different attacks such as routing attacks, impersonation, DOS etc. Whereas, in passive attacks the intruder overhears network traffic without active participation in the network operations. Eavesdropping is an example of passive attack (Aljumah, 2015).

#### 4. DOS attacks in MANETs

The DOS is MANETs aims to interrupt the availability of a certain node or even the entire network by jamming the network signal or exhausts the battery resources of the nodes. There are two general types of DOS attacks; (i) those crashes the services (ii) those floods the services. DOS attacks can be launched against any protocol layer (Uddin et al., 2013). On the lower layers of the protocol set such as MAC and physical layer, the attacker can use the signal jamming approach to block the communication channels. On the middle network layer, the attacker can manipulate the routing protocol and disrupt the whole traffic. Whereas, on the upper layer such as application layer, the attacker can add the malicious data packets which degrades and delays the performance of the services to a great extent (Ahamad and Aljumah, 2014). Types of DOS attacks are jamming, flooding, DDOS (Distributed- Denial-of-Service), sleep deprivation, RREQ (Repeated Requests) etc.

#### 5. IDS in MANETs

MANETs consists of wireless mobile nodes which communicate through wireless links. There are certain limitations in the type of network such as short battery life, bandwidth constraints, security etc. Security is considered a main concern with respect to MANETs. Due to wireless communication links, dynamic changing topologies, the networks are vulnerable to variety of attacks such as node compromise, eavesdropping, DOS, routing attacks. The identification of these types of attacks is a challenging task. Intrusion detection is an adequate way to identify such type of attacks in MANETs (Wanlei, 2012). The IDS is an extensive approach which continuously monitors the network activities and takes the appropriate action when needed. According to the data collection and detection mechanism, the IDSs are classified into following categories; (i) signature based, (ii) anomaly based and (iii) specification based. In signature based IDS a priori knowledge is used to detect the known attacks on the network. There is a drawback in this kind of

scheme that it cannot be applied to unknown attacks. In anomaly based IDS the system behavior is monitored, if it deviates from the normal behavior by a certain threshold, the anomaly is detected. In specification based IDS, certain constraints are set for the operations or protocols (Tan and Seah, 2005). The IDS monitors the functioning according to the constraints.

#### 6. IDS architecture

The current IDS architecture of MANET consists of three taxonomies; (i) stand-alone, (ii) co-operative, and (iii) hierarchical. In stand-alone architecture every node is responsible for its own security without any collaboration with the rest of the nodes in the network. On the other hand, in co-operative based architecture, the nodes have their own IDS systems (Arunmozhi and Venkataramani, 2011). They co-operatively decide about the intrusion in the network by sharing information and parameters. Whereas, in third type of architecture which is hierarchical based, the network is divided into clusters and particular nodes are chosen based upon a certain criteria as CHs cluster heads who takes the responsibility and roles in performing the intrusion detection. The primary advantage of this type of architecture is the adequate utilization of the resources, but has a disadvantage of selecting a node as a CH which is impractical in ad-hoc networks (Redwan and Kim, 2008), where the nodes move freely in all directions.

#### 7. IDS issues in MANETs

AS discussed above MANETs are more susceptible to attacks than their wired counterparts, because of wireless medium, limited bandwidth, very less infrastructure or none, limited battery power, scarce memory resources. Keeping the above limitations in mind, applying IDS on these types of networks is a very demanding and costly matter. Since, most of the IDS are designed for wired networks, so, it is impractical to implement these solutions directly in MANETs. The researchers and experts in the field are busy in developing new or modifying the existing schemes to fit into the MANETs. The characteristic of MANETs forces the IDS systems to be distributed and shared. With the possibility of increase in the attacks on the MANETs, the researchers' focuses more on anomaly type IDS in the literature.

#### 8. Proposed solution

In the recent time, with the enormous growth of internet and network technology, the intrusion detection, prevention and defense methods have attained a great speed. The main purpose of an IDS to identify and stipulate probable security issues and breakdowns in the system. An IDS survey report is mentioned in (Xenakis et al., 2011) and there are

some of the selected IDS that have their base on forensic analysis (Guo and Simon, 2010).

The first and most important assumption of this research is that to have existing IDS, Flexible Mobile Adhoc Network IDS (Sharma et al., 2012). The application of analyzed forensic log data and adequate report generation is the back bone of flexible mobile adhoc network intrusion detection system. Two categories of the nodes are assumed by in the proposed IPAM (intrusion Prevention Algorithm in MANET): normal mobile ad-hoc nodes and Intrusion detection nodes- where the existing MANET infrastructure is used by these IDS nodes to create the management network. After a defined thresh hold time all the selected IDS nodes send the

collected information packets to the main IDS station that is related to the network activities. Following this procedure, the merged log file data is manipulated using forensic analysis and a report is generated. The data information is contained in these log files of packet level like packet size, packet type, node ID, event type, routing protocol info and time stamps. The algo that is being used for forensic analysis uses elimination method where the results are retrieved in the form of IDS repetition's using a pool of consecutive log search procedures. So, based on such existing IDS models, I have made an attempt to improve its functionalities and prepared a prevention technique for DDoS attacks. Fig. 1 illustrates the security system.

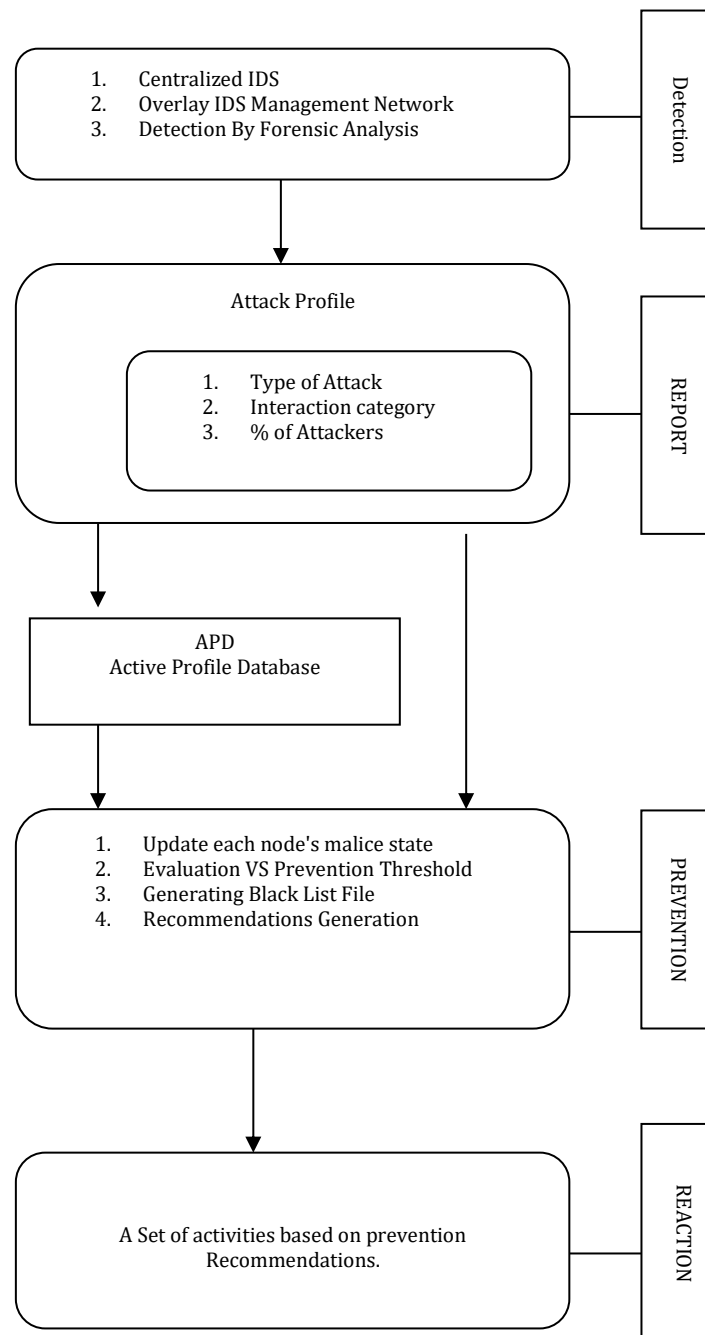


Fig. 1: Proposed security system overview

A schema of IDS analysis is provided by the report and these can be just an instance of the future

of the overall assessment for a specific period of time of the network security. A set 'R' that maintaining the

list of detected malicious nodes, their attack description that in turn provide the attack information like type of attack, interaction category (Active-Passive), the detected attackers list and it is easily possible to generate an APD (Active Profile Database) after statistically analyzing the occurrence and behavior of the attacker nodes. This active profile database can provide a statistical analysis of characteristics of every malicious node for longer period. These results generate the possibility to access the vital information to prevent the future similar attacks. The iterative screening of every network node is done with the inclusion of the report generated by IDS module.

DDoS attacks main aim is to decrease the performance of the network specifically service and resource accessibility and using APD, we can get

organized proof of nodes being malicious and magnitude of the attack and a report will be generated after every IDS cycle. Every modification in the existing value of detected malicious nodes will invoke the update scheme of the active profile database. One of the main aims of our proposed mechanism is to provide an iterative and adaptive security system that knows all the new updates. Therefore, having this characteristic, the proposed solution will have an organized list of nodes ordered as per their malicious magnitude called a blacklist table. The proposed algorithm and flowchart of the prevention system is illustrated in the Fig. 2. The preventive threshold is a given integer and is represented by  $\Psi$  and represents the highest value after which a malicious node will be blacklisted.

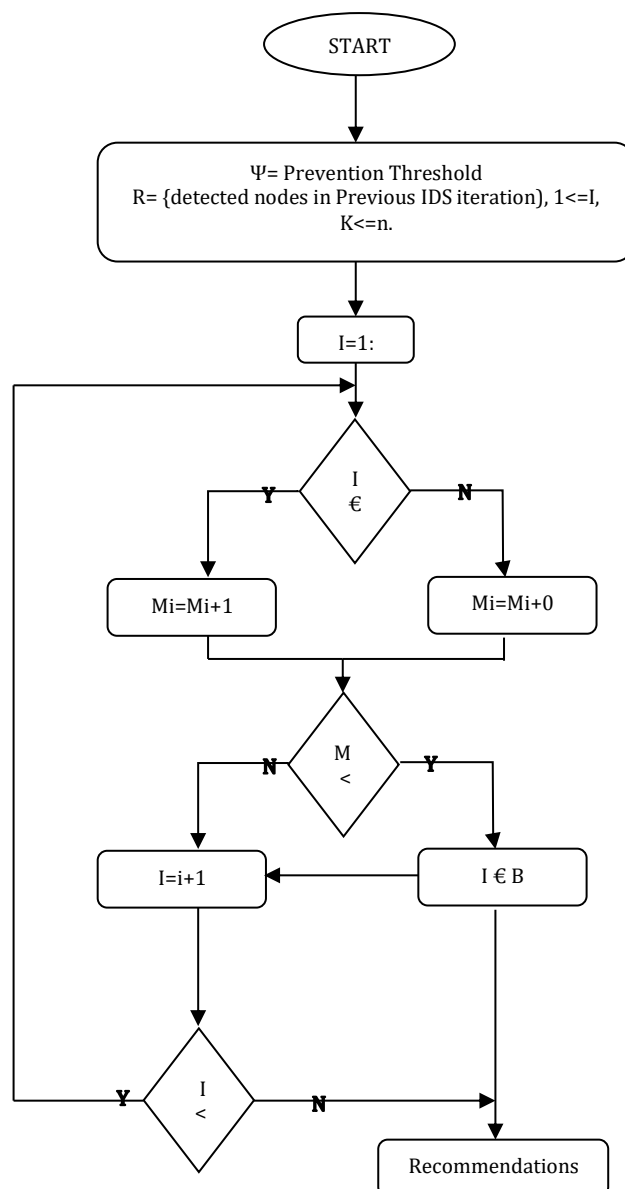


Fig. 2: Proposed IPAM algorithm flowchart

The set of nodes that were diagnosed as malicious in the foregoing Intrusion Detection System's iteration is represented by R. every member of R is identified by their associated node ID and those node IDs are used for future analysis. N is

the number of nodes of the assumed network and APD maintains the track record of malicious magnitude status number of each node represented by M. So, whenever a node with ID I is diagnosed with malicious character its Mi number is the active

profile database will be incremented else the table will maintain the same value of Mi. In case the Mi number is greater than the threshold number fixed in  $\Psi_p$ , then the node IDs will be added as a new entry to the table of black listed IDs' represented as 'B'. Proposed preventive procedure will produce and forward a recommendation to the reactive module regarding what must the system should do in order to defend and maintain the security and performance of the network. Blacklist table nodes (value  $> \Psi_p$ ) are considered with higher possibility of being malicious. As a defensive measure, the system's responsive scheme, the functionality of these selected nodes will be decreased and labeled as untrustworthy and will be isolated from playing any role in creating any part of the network route and in some critical conditions these nodes are declared as incompetent and are isolated from the network fully. Since the report generated by intrusion detection system comprehends the probability to get the information of the activity of some nodes, these nodes are marked in the blacklist table and their functionality and activities are monitored and evaluated as a member of team and as a team as well. The response procedure will have schematic functions which are utilized in some situations of the attack occurrence that is based on the information response perceived by the prevention scheme and are interdependent conjointly. One of the aims of this proposed architecture is to enhance or at least maintain the performance of the MANET in presence of attack and if there is any change is the blacklist table, prevention mechanism will invoke the reaction module and the most serious prevention suggestion would be to isolate them for doing any network activity.

## 9. Code for simulation

The code that has been used for the simulation purpose in this work is as follows:

```
boolcheckNode();
int phi=20; //phi being prevention threshold, 10 is a token
value
usingnamespacestd;

void main()
{
    inti=0;
    int M=0;
    int k=0;
    bool res=false;

    res=checkNode();

    if(res)M+=1;
    else
        M+=0;

    if(M<=phi)
    {
        cout<<"\n Entered node is
among Black Listed node ";
```

```
    }
    else
    {
        i+=1;
        if(i<=k)res=checkNode();
        else
            {
                //steps to be discussed (future)
            }

    //return 0;
    }
}

boolcheckNode()
{
    int list[10]={ 6,9,11,41,43,47,61,64,59,93}; //list of infected
nodes(R)
    int node, pos=0;
    bool found=false;

    cout<<"enter node number ";
    cin>>node;
    for(int i=1;i<=10;i++)
    {
        if(list[i]==node) found=true;
        pos++;
        break;
    }
    if(found==true)
        cout<<"Malicious node found at
"<<pos<<" position\n";
    else
        cout<<"No Malicious node found\n";
    system("pause");
    return 0;
}
```

## 10. Simulation and results

To carry out simulation we used NS-2 network simulator and trace graph analyzer to obtain results. The first assumption made to start simulation is that the malicious intruders were detected by the IDS using FMIDS algo (Uddin et al., 2013) that fetches log file using forensic analysis in x iterations at maximum. The detected set of malicious nodes becomes narrow after every iteration by the inclusion of n new exclusion criteria and after the final iteration is completed by IDS, the final set R is generated. IDSIN represent the exact IDS iteration (loop) and in the experiment performed in this research.  $N \in \{1, 2, \dots, 6\}$  represents the six contiguous iterations that in turn are utilized to generate the report.

Every IDSIN can be the cause of invoking the Intrusion Prevention Algorithm in MANET (IPAM). The report generated by IDS is utilized as input data to create the blacklist file and the prevention procedure recommendations are generated. Our network is comprised of 200 nodes and the area is confined to 600m<sup>2</sup> for simulation that include the early distribution of randomly and uniformly nodes with 300 m transmission range. For routing we

chose AODV protocol and for MAC we chose IEEE802.11 protocol. Two ray reflection models are used to illustrate the propagation. The authentic data traffic is simulated using two FTP sources have the following details shown in Table 1 including IS = Ingress rate, PS= Packet Side and WS = Window size (default).

**Table 1:** L Simulated traffic details

PS	1600 bytes
WS	21
IS	0.5 Mbs

The Constant Bit Rate (CBR) source are used to simulate the attack traffic having 512 bytes packet size and 0.0005s arrival time followed by a collaborative and integrated action towards the same target. The network with 10 and 20 attackers have been used for simulation of ten CBR sources having dissimilar inter-advent time and packet sizes along with different time of source activity are used to simulate the background traffic. The experiments implicitly imply integrated and repetitive action of 10 and 20attacks throughout the following three intervals of time shown in Table 2.

**Table 2:** Time intervals of attacks

1	0.1Ts - 0.3Ts
2	0.4Ts - 0.6Ts
3	0.7Ts - 0.9Ts

Where Ts is the simulated network activity's time duration (10 lcontinuous same intervals of time). Six contiguous forensic analysis iterations are used to perform the IDS analysis and everyone providing explicit and accurate set of suspicious nodes and concluding with generation of set R. The entire mechanism can be implemented and executed over the complete simulation period or on some specific slots of time which can certify the occurrence of attacks or presence of attackers.

The results obtained after 6 IDSIN iterations considering 10 equal IDS activity intervals of time is illustrated in Figs. 3 and 4 including the complete simulated network scenario for 5 % and 10 % attackers. It is the indication of isolation of three intervals of action initiated by a group of nodes. The detected nodes set in our simulation case include the following IDs{6,9,11,41,43,47,61,64,59,93} and {11, 17, 22, 29, 37, 43, 52, 59, 64, 71, 77, 82, 84, 88, 91, 96, 99, 102, 111, 119, 121} 5% and 10 % intruders network respectively.

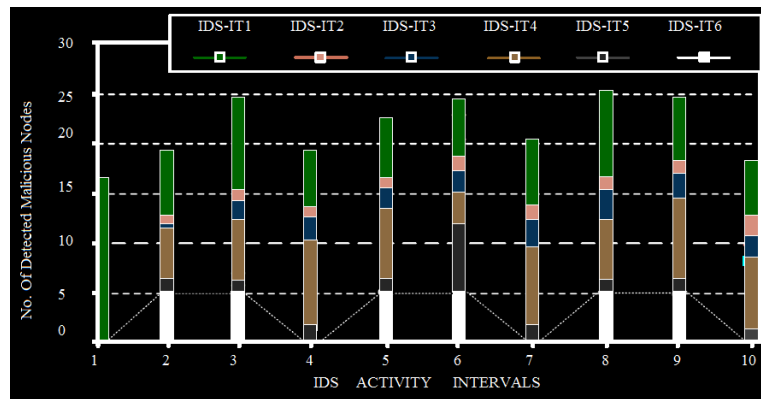


Fig. 3: Detected malicious nodes in MANET with 5% Attackers

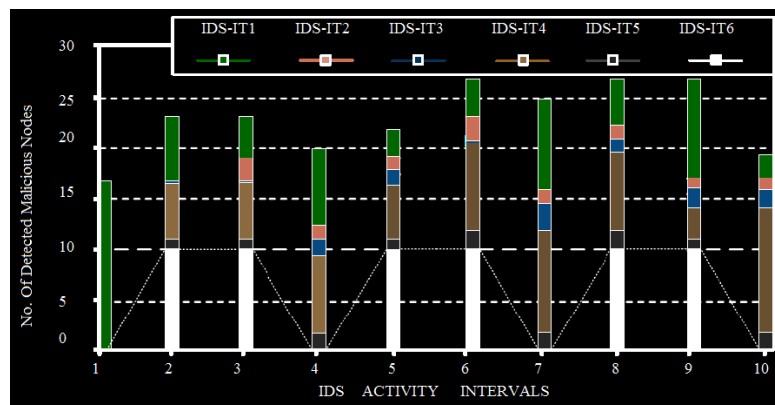


Fig. 4: Detected malicious nodes in MANET with 10% attackers

Intrusion Prevention Algorithm in MANET (IPAM) will increment the MI for detected nodes. Therefore, 3 continuous attacks were detected that were initiated by a group of nodes' synchronous activity. After the first detected malicious group attack FMIDS is allowed to generate report even if the examination of whole simulated data is not completed, active profile database can be easily

updated and authorize IPAM to begin the blacklist update. In case IPAM procedure has made any update to the blacklist file, then these updates are instantly forwarded to the reactive module that in turn can respond as per the received recommendations. As a requirement of this research, we have assumed that the blacklist file gets updated after each detected group attack. For the malicious



settings for prevention, these set of nodes will form the blacklist and the specified nodes will be isolated and excluded from further network communications as per the recommendations. So, as output, two more attacks that were detected can be defended and prevented.

## 11. Conclusion

The Magnitude of DDoS and therefore harm as escalated with the inclusion of various different attack sources and therefore creating suitable environment for harming the security and performance of the network. The influence of attack and its frequency can further worsen the network performance and prevent the legitimate users of the network from accessing the network services. This article stresses in the possible security technique and proposed a prevention scheme that is favorable to be applied in MANETs that are vulnerable to DDoS attacks. Based on the basic structure and functions of existing IDS, we have sued results in the proposed algo in a manner pertaining to time. Proposed prevention algo is a multiway adaptable administratively and technically for various security needs and is also adjustable according to the existing information simultaneously updatable blacklist table. Following this can lead to generate recommendation for reaction module and thus approaching to assure the network performance, security and survivability at the time of attack occurrence.

## Acknowledgement

This research was funded and conducted at Prince Sattam bin Abdulaziz University, Alkharj, Saudi Arabia during the academic year 2016/2017 under research number 2017/01/7396.

## References

- Aad I, Hubaux JP, and Knightly EW (2008). Impact of denial of service attacks on ad hoc networks. *IEEE/ACM Transactions on Networking*, 16(4): 791-802. <https://doi.org/10.1109/TNET.2007.904002>
- Ahamad T and Aljumah A (2014). Hybrid approach using intrusion detection system. *International Journal of Engineering Research and Technology*, 3(2): 197-208.
- Ahamad T and Aljumah A (2015). Detection and defense mechanism against DDoS in MANET. *Indian Journal of Science and Technology*, 8(33): 1-4.
- Aldaej A and Ahamad T (2016). AAODV (Aggrandized Ad Hoc on demand vector): A detection and prevention technique for manets. *International Journal of Advanced Computer Science and Applications*, 1(7): 132-140.
- Alicherry M, Keromytis AD, and Stavrou A (2009). Evaluating a collaborative defense architecture for manets. In the *IEEE International Conference on Internet Multimedia Services Architecture and Applications (IMSAA'09)*, IEEE: 1-6. <https://doi.org/10.1109/IMSAA.2009.5439498>
- Aljumah A (2015). Detecting distributed denial of service (Ddos) attack using TTLv constraint in mobile adhoc networks (MANET). *Science Internationals*, 27(6): 5037-5040.
- Aljumah A and Ahamad (2016). A novel approach for detecting DDoS using artificial neural networks. *International Journal of Computer Science and Network Security*, 16(12): 132-138.
- Arunmozhi SA and Venkataramani Y (2011). A new defense scheme against DDoS attack in mobile Ad Hoc networks. *Communications in Computer and Information Science*. Springer Berlin Heidelberg, 133: 210-216.
- Guo Y and Simon M (2010). Network forensics in MANET: Traffic analysis of source spoofed DoS attacks. In the *4<sup>th</sup> International Conference on Network and System Security (NSS'10)*, IEEE, Melbourne, Australia: 128-135. <https://doi.org/10.1109/NSS.2010.45>
- Nadeem A and Howarth M (2009). Adaptive intrusion detection and prevention of denial of service attacks in MANETs. In the *International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*, ACM Leipzig, Germany: 926-930.
- Redwan H and Kim KH (2008). Survey of security requirements, attacks and network integration in wireless mesh networks. In the *conference on New Technologies, Mobility and Security (NTMS'08)*, Tangier, Morocco, IEEE: 1-5. <https://doi.org/10.1109/NTMS.2008.ECP.94>
- Sharma P, Sharma N, and Singh R (2012). A secure intrusion detection system against DDOS attack in wireless mobile Ad-hoc network. *International Journal of Computer Applications*, 41(21): 16-21.
- Tan HX and Seah WK (2005). Framework for statistical filtering against DDoS attacks in MANETs. In the *Second International Conference on Embedded Software and Systems*, IEEE, Xian, China: 1-8. <https://doi.org/10.1109/ICCESS.2005.57>
- Uddin M, Alsaqour R, and Abdelhaq M (2013). Intrusion detection system to detect DDoS attack in gnutella hybrid P2P network. *Indian Journal of Science and Technology*, 6(2): 4045-4057.
- Wanlei Z (2012). Keynote: Detection of and defense against distributed denial-of-Service (DDoS) attacks. In the *IEEE 11<sup>th</sup> International Conference on Trust, Security and Privacy in Computing and Communications*, IEEE, Liverpool, UK. <https://doi.org/10.1109/TrustCom.2012.341>
- Xenakis C, Panos C, and Stavrakakis I (2011). A comparative evaluation of intrusion detection architectures for mobile ad hoc networks. *Computers & Security*, 30(1): 63-80.
- Xiang M, Chen Y, Ku WS, and Su Z (2011). Mitigating DDoS attacks using protection nodes in mobile Ad Hoc networks. In the *IEEE Conference on Global Telecommunications*, IEEE, Houston, USA: 1-6. <https://doi.org/10.1109/GLOCOM.2011.6134032>