Enhancing Cyber Security in Modern Internet of things (IoT) Using Intrusion Prevention Algorithm for IoT (IPAI)

Abdulaziz Aldaej

College of Computer Engineering & Sciences
Prince Sattam Bin Abdulaziz University, Saudi Arabia

Abstract
A prevention technique is proposed to enhance cyber security of IoT devices and networks against DDoS attacks which consume the bandwidth in modern Internet of things (IoT) devices. 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 in IoT devices 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.

Keywords:
IoT, DDoS, Cyber Security, IDS, IPS.

1. Introduction

The Internet of Things (IoT) is a developing global trend in the internet-based data architecture facilitating the exchange of goods and services in the global supply chain network. IoT is an application domain integrating diverse technologies and social arenas[1]. [2]has described IoT as "A network of things, every one of them embedded with wireless sensors and connected through the world wide web". The fundamental aim is to ensure diverse range of things that can be connected and operated such that they can interact with themselves and users. It is an active IT infrastructure having self-configuring ability for establishing interoperable communication protocols between physical and virtual identities of things through intelligent interfaces[3].IoT supports bilateral continuous exchange of sensed data and information about the environment and automatically triggering actions as per the real-world events [4] One of the major challenges faced by IoT world is not expansion but its security. As we all know traditional wired networks are relatively more secure than their wireless IoT 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 [1]. So, these networks are well equipped against any type of intrusion or Denial of Service (DOS) attacks. On the other hand, the IoTs also known as peer-to-peer networks are wireless in nature, and are inherently vulnerable to different types of attacks [2]. 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 [3]. So, it is necessary for each communicating node to incorporate some kind of security mechanism to prevent any kind of attacks.

2. Vulnerabilities' in IoTs

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 [4]. IoT's 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 [5]. 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 [6]. Every contributing element in the IoT networks is susceptible to internal as well as external threats. As, a result the IoTs require robust security scheme to ensure the network security.

3. Attacks in IoTs

There are mainly two types of attacks in IoTs; which are internal and external attacks. The internal attacks are far more dangerous than the external attacks. In the internal

Manuscript received January 5, 2026
Manuscript revised January 20, 2026
https://doi.org/10.22937/IJCSNS.2026.26.1.8

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 [7]. 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 [8]. 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, DDoS etc. Whereas, in passive attacks the intruder overhears network traffic without active participation in the network operations. Eavesdropping is an example of passive attack [9].

4. DDoS Attacks in IoTs

The DDoS is IoT's 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 DDOS attacks; (i) those crashes the services (ii) those floods the services. DDOS attacks can be launched against any protocol layer [10]. 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 [11].

5. IDS in IoTs

IoT's 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 IoT environment. Due to wireless communication links, dynamic changing topologies, the networks are vulnerable to variety of attacks such as node compromise, eavesdropping, DDoS, 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 IoT [12]. 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 [13]. The IDS monitors the functioning according to the constraints.

6. IDS Architecture

The current IDS architecture of IoT 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 [14]. 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 [15], where the nodes move freely in all directions.

7. IDS issues in IoT

AS discussed above IoTs 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 IoTs. The researchers and experts in the field are busy in developing new or modifying the existing schemes to fit into the IoTs. The characteristic of IoTs forces the IDS systems to be distributed and shared. With the possibility of increase in the attacks on the IoTs, 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 [16] and there are some of the selected IDS that have their base on forensic analysis [17].

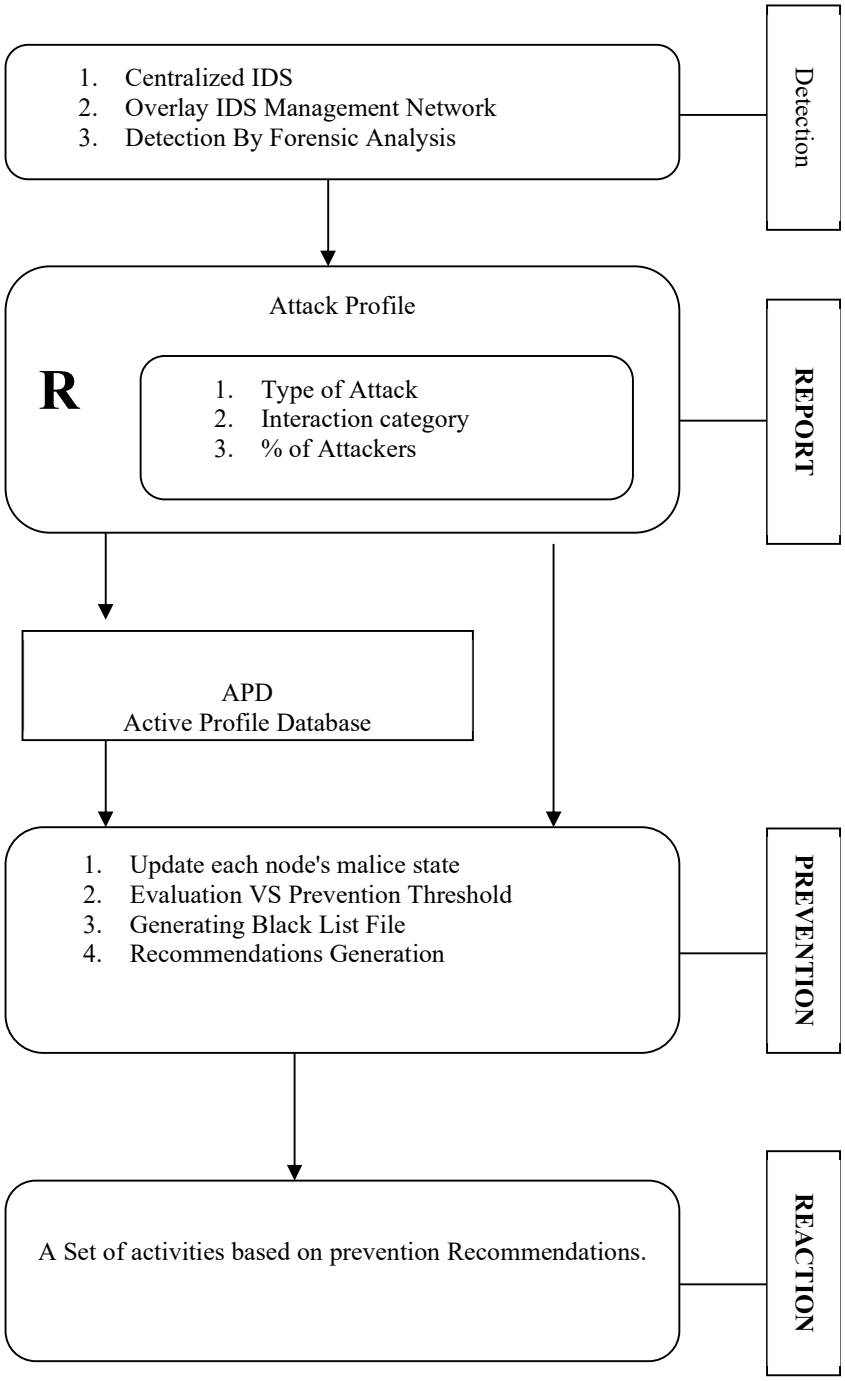

Figure 1: Proposed Security System Overview

The first and most important assumption of this research is that to have an existing IDS, Flexible Internet of things IDS [18]. The application of analyzed forensic log data and adequate report generation is the back bone of flexible IoT intrusion detection system. Two categories of the nodes are assumed by in the proposed IPAM (intrusion Prevention Algorithm in IoT): normal IoT nodes and Intrusion detection nodes– where the existing IoT 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. Figure 1: illustrates the security system.

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 discription 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 is knowing 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 figure 2. The preventive threshold is a given integer and is represented by Ψ and represents the highest value after which a malicious node will be blacklisted.

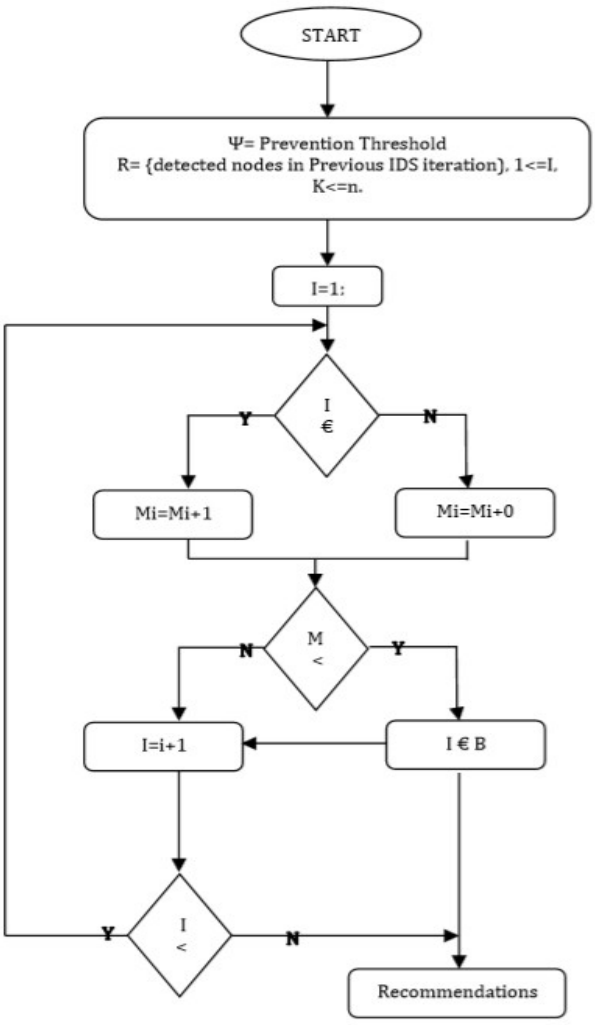

Fig. 2: Proposed IPAM algorithm flowchart

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 Ψp, 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>Ψp) 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 IoT network 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

```
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

The first assumption made to start simulation is that the malicious intruders were detected by the IDS using FMIDS algo [10] 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. Nε {1,2,,,6}represent 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 IoT (IPAI). 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 600m2 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 model is 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. 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 continuous 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.

Figure 3. Detected malicious nodes in IoT with 5% Attackers.

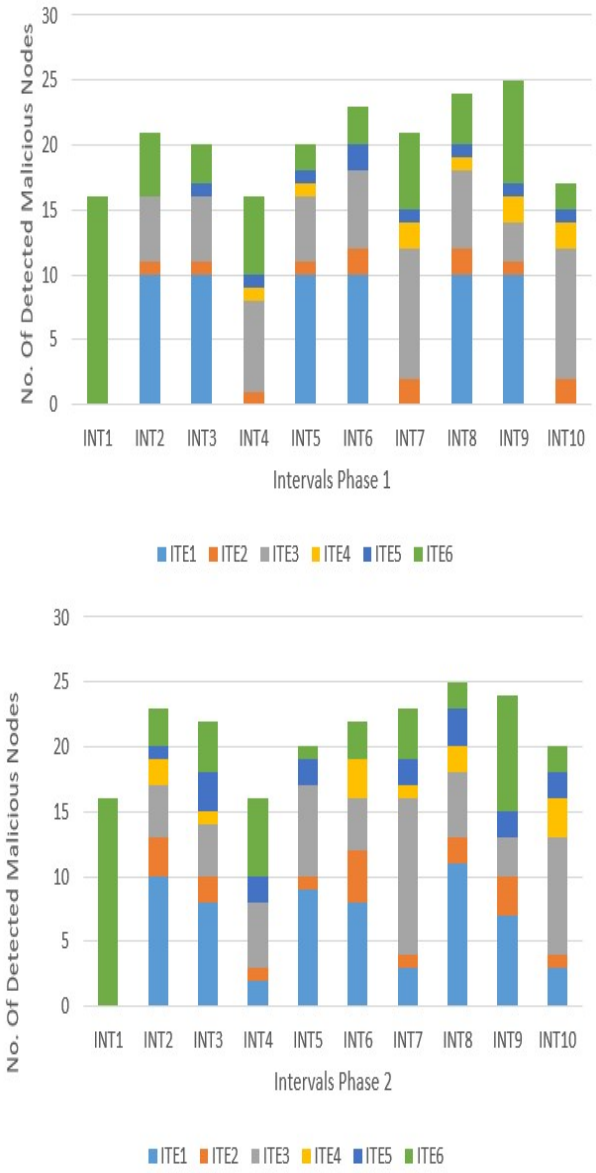

Figure 4. Detected malicious nodes in IoT with 10% Attackers.

The results obtained after 6 IDSIN iterations considering 10 equal IDS activity intervals of time is illustrated in figure 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} 5% and 10 % intruders network respectively.

Intrusion Prevention Algorithm in IPAI (IPAI) 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 IPAI to begin the blacklist update. In case IPAI 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 IoT technology. 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 IoT networks 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 conducted at Prince Sattam bin Abdulaziz University, Alkharj, Saudi Arabia during the academic year 2018.

References

[1] T. A. Ahanger and A. Aljumah, "Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms," in IEEE Access. doi: 10.1109/ACCESS.2018.2876939
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8519613&isnumber=6514899

[2] Ahamad Ahanger, Tariq. (2018). Defense Scheme to Protect IoT from Cyber Attacks using AI Principles. International Journal of Computers Communications & Control. 13. 915-926. 10.15837/ijccc.2018.6.3356.

[3] K. Rose, S. Eldridge, and L. Chapin, "THE INTERNET OF THINGS: AN OVERVIEW, Understanding the Issues and Challenges of a More Connected World," 2015.

[4] R. H. Weber, "Internet of Things – New security and privacy challenges," Comput. law Secur. Rev., vol. 26, pp. 23–30, 2010.

[5] Abdullah Aljumah, Tariq Ahamad,"A Novel Approach for Detecting DDoS using Artificial Neural Networks". International Journal of Computer Science and Network Security, 132 VOL.16 No.12, December 2016.

[6] Abdulaziz Aldaej and Tariq Ahamad, "AAODV (Aggrandized Ad Hoc on Demand Vector): A Detection and Prevention Technique for Manets" International Journal of Advanced Computer Science and Applications(IJACSA), 7(10), October 2016.

[7] M. Xiang, Y. Chen, W. S. Ku and Z. Su, "Mitigating DDoS Attacks Using Protection Nodes in Mobile Ad Hoc Networks," Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE, Houston, TX, USA, 2011, pp. 1-6.

[8] Tariq Ahamad, Abdullah Aljumah," Detection and Defense Mechanism against DDoS in MANET", Indian Journal of Science and Technology, Vol 8, No 33, December 2015

[9] I. Aad, J.P. Hubaux, E.W. Knightly, "Impact of Denial of Service Attacks on Ad Hoc Networks," IEEE/ACM Transactions on Networking (TON), vol. 16 (4), pp. 791-802, 2008.

[10] A. Nadeem and M. Howarth, "Adaptive Intrusion Detection & Prevention of Denial of Service Attacks in MANETs," International Conference on Communications and Mobile Computing, Leipzig, Germany, 2009.

[11] M. Alicherry, A. D. Keromytis, and A. Stavrou, "Evaluating a Collaborative Defense Architecture for MANETs," IEEE Workshop on Collaborative Security Technologies (CoSec), December 2009.

[12]Ahamad T, Aljumah A. "Detection and Defense Mechanism against DDoS in MANET", Indian Journal of Science and Technology. 2015 Dec Vol 8(33).

[13] Aljumah A, " Detecting Distributed Denial Of Service (Ddos) Attack Using TTLv Constraint In Mobile Adhoc Networks (MANET) ", Science Internationals, 2015 Dec Vol 27(6),5037-5040.

[14] Uddin M, Alsaqour R, Abdelhaq M. Intrusion detection system to detect DDoS attack in gnutella hybrid P2P Network. Indian Journal of Science and Technology. 2013 Feb; 6(2):71–83.

[15] Ahamad T, Aljumah A," Hybrid Approach Using Intrusion Detection System", International Journal of Engineering Research & Technology, Vol. 3 Issue 2, February - 2014

[16] Wanlei, Z. (2012). Keynote: Detection of and Defense Against Distributed Denial-of-Service (DDoS) Attacks. 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), (1),

[17] Hwee-Xian Tan and W. K. G. Seah, "Framework for statistical filtering against DDoS attacks in MANETs," Embedded Software and Systems, 2005. Second International Conference on, 2005

[18] Arunmozhi, S. A., & Venkataramani, Y. (2011). A new defense scheme against DDoS attack in mobile Ad Hoc networks. In Communications in Computer and Information Science (Vol. 133 CCIS, pp. 210–216)

[19] H. Redwan and K. H. Kim, "Survey of Security Requirements, Attacks and Network Integration in Wireless Mesh Networks," New Technologies, Mobility and Security, 2008. NTMS '08., Tangier, 2008, pp. 1-5

[20] C. Xenakis, C. Panosb, I. Stavrakakisb, "A comparative evaluation of intrusion detection architectures for mobile ad hoc networks", Computers & Security, vol. 30, no. 1, pp. 63–80, 2011.

[21] Guo, Y., & Simon, M. (2010). Network forensics in MANET: Traffic analysis of source spoofed DoS attacks. In Proceedings - 2010 4th International Conference on Network and System Security, NSS 2010 (pp. 128–135).

[22] Sharma, P., Sharma, N., & Singh, R. (2012). A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network. International Journal of Computer Applications, 4121, 975–8887. doi:10.5120/5824-8064