Protection against Denial of Service in Automation Systems

Farag M. Afify
Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt

Hamdy M. Kelash, Osama S. Faragallah, Maha S. Tolba
Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt

Hala S. El-Sayed
Faculty of Engineering, Menoufia University, Shebin El-kom, Egypt

ABSTRACT
Denial of service (Dos) problem has great impact on all devices in automation system. A lot of techniques have been developed that can protect systems from Dos attack. This paper presents some proposal solutions to solve this problem in order to decrease the risk factor by Using Trusted Authentication Device, Counter, and connecting the network with two routers. The first router is the basic and the other one is reserve. Then, dividing the devices into normal and vip devices, connecting vip devices with two networks, Trust Point (TP) to prevent attackers from access to AS and the optimal solution mixing between the previous ones.

Keywords
Automation Systems, Trusted authentication device, trusted point, Counter, Monitoring the Source IP addresses and network topology.

1. INTRODUCTION

Automation Systems (AS) are devices connected in a network of hardware and software, which controls and observes all sub systems like (HVAC, Lighting, Fire Alarm, Elevators, etc.) . AS guarantees the best performance of the devices save time and energy and reduces operating costs as well as the comfort and safety of building occupants. A technical infrastructure is necessary to fulfill the previous demands.

AS. is found where mechanical equipment, electrical systems and other equipments in building are joined with microprocessors that communicates with each other and to a computer. All devices in the automation system can be remote accessed through a computer, enabling the manager to view or control the system of the appliances from virtually any location through the internet.

The goal of the automation system is to make buildings as ”intelligent” as possible .Centralized in this concern means that automatic control is done by a single controller or control station.

AS has two levels of architecture as shown in Figure 1, the two-level architecture consists of a control network level and a common backbone which together form the automation network (AN). The control network is connecting the field devices. It has small bandwidth in the order of a few K bit/s. The management devices cannot be connected through this control network, control sub networks and management devices are connected via a high-bandwidth backbone network and this network is used to connect AS and foreign networks (e.g. Internet).

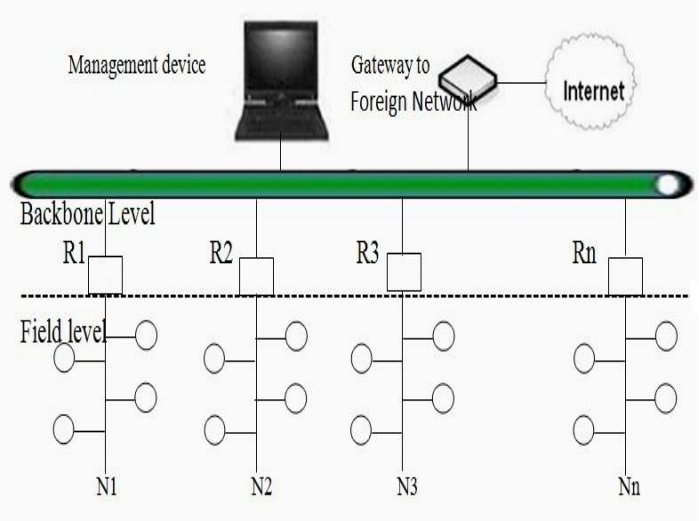

Fig. 1: Automation System Architecture

Automation systems have a lot of attacks, these attacks have two types 1- Passive attacks – eavesdropping on or monitoring of transmissions (ex. Release of message contents and Traffic analysis) 2- Active attacks – modification of the data stream or creation of a false stream (ex. Masquerade , Replay, Modification of message and Denial of service).

2. DOS AND TYPES OF ATTACKS

Automation systems require automatic information interchange among all system devices. We must create a secure environment which involves specifying a policy containing particular security demands .There are security attacks on automation system. Some of these attacks can be prevented through encryption, authentication and firewall techniques. There are some attacks which cannot be prevented by using Encryption and Authentication methods like Denial of service (Dos) attacks. DoS. Attack is an attack on network, software and hardware of the system that make system or network(s) incapable of doing the functions designed to be performed, or to make the system services unavailable and prevent users from access to the system .Attackers can succeed to Dos by using network flooding, redirection, code injection and physical attack.

The first method is Flooding: flood the network, the attacker send packets to achieve not leaving enough bandwidth for the normal packets. [1]

The other method is to crash a hardware or software item and make it Unusable. Servers, routing devices are the common targets that could be damaged during an attack.

2.1 DoS. Attacks

Table 1: Attacks, Affected Area and Description

	Attack	Affected Area	Description
1	Network level Device	Routers, IP Switches, Firewalls	Attack attempts to exhaust hardware resources using multiple duplicate packets or a software weakness.
2	OS Level	Equipment Vendor OS, End-User Equipment.	Attack takes advantage of the way operating systems implement protocols.
3	Applicatin Level Attacks	Application software	Attack a service or machine by using an application attack to exhaust resource.
4	Data Flood (Amplification ,Oscillation, Simple Flooding)	Network	Attack in which massive quantities of data are sent to a target with the intention of using up bandwidth/processing resources.
5	Protocol Feature Attacks	Servers, Client PC	Attack in which weakness in protocol are used to take down network resources. Methods of attack include: IP address spoofing, and corrupting server cache.

In a denial of service, attackers may do attacks from a single device or from multiple devices that they control. When attackers attack systems from multiple devices or places that are distributed in the network, it is called a distributed denial of service (DDos) attack. But when attackers attack systems from a single device or place, it is called a single-source denial of service (SDos) attack. DDos attacks have strong impact than SDos attacks, because of the amount of bandwidth, CPU, memory that can be affected. In practice, protecting systems against DDos attacks is proven to be harder than defending against SDos attacks.

A Dos brute-force attack aims to prevent users from accessing to the service by sending a vast amount of seemingly valid service requests and trying to exhaust a key resource of the system. For example, in a User Datagram Protocol (UDP) flood attack, an attacker sends a high number of UDP segments to random devices on a system to consume its bandwidth; this makes systems not available to other users. [2]

3. DOS. DETECTION AND COUNTERMEASURES

3.1 Detection

The most useful ways in the process of detect Dos are called intrusion detection systems (IDS).The main goal of IDS is to detect the misuse of the system by monitoring operations occurring in a computer system or network, prevent attempts to gain unauthorized access to a network or to create network degradation and analyze all operations which might be signs of possible incidents. They are imminent threats of violation of computer security policies, acceptable use policies, or standard security practices.

Intrusion detection systems (IDS) primarily focus on identifying possible incidents, logging on information about them in order to stop them, and report them to security administrators. In addition, companies use IDSs in a lot of purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies.

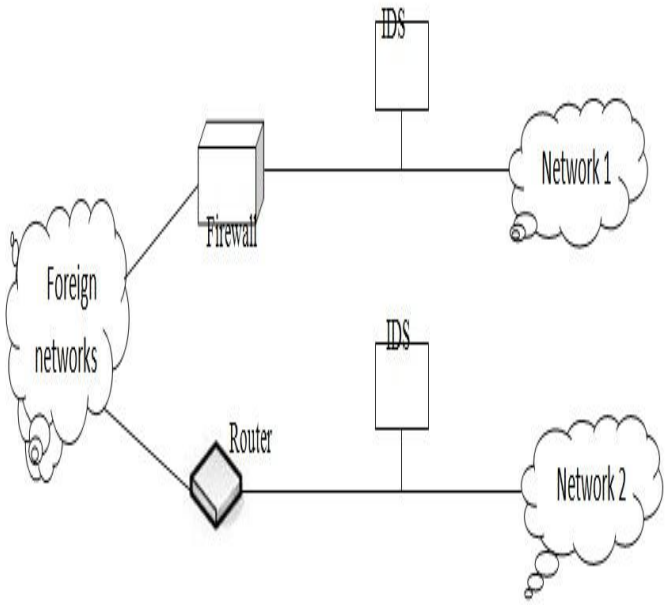

Fig. 2: IDS can be connected in network with or without firewall

3.2 Counter Measures

After a Dos attack has been detected by the IDS, system must deactivate the port where a Dos attack has been detected and stay current with patches and security updates. You should configure your applications, services, and operating system with denial of service in mind, activate the TCP/IP stack against denial of service. You should make sure your account lockout policies cannot be exploited to lock out well known service accounts, make sure your application is capable of handling high volumes of traffic and that thresholds are in place to handle abnormally high loads. Lastly, review the applications which the system fail to do , use a network Intrusion Detection System (IDS) because these can automatically detect and respond to attacks.IDS must have

these features (high detection rates, low false negative alarms, low false positive alarms and quick detection rates) and use resource and bandwidth throttling techniques.

3.3 Prevention

Prevention of Dos Requires the Following Actions:

1- High redundancy and high availability network design.

2- Perimeter Defence - Any packets must pass through firewalls to reach internal network.

3- Defence In-depth - Intruder Detection System (IDS) will allow detection and take action to remove infected packets. IDS may be able to detect known attacks but not new ways of these attacks.

4- Malware detection and prevention.

5-Periodic Scanning- Periodic network scanning will detect weakness host and detect new attacks.

6-Keeping the system up to date with patches or version upgrades, closing old services, applying Access Control Lists on the system and changing passwords every period and applying good password policies.

4. RELATED WORK

4.1 Virtual Bridges

By using Virtual bridges , we will decrease risk factor as shown in Figure 3 . For example, the virtual bridge VB2 that is put in N2. This virtual bridge decreases the Dos-RF of all devices to 4 and alternative communication paths have to be provided by using redundant interconnections between virtual bridges and devices, for example, a redundant connection is added between VB2 and R2. Using this connection, the devices of VN22 are still able to connect with other networks. Applying this case, the Dos-RF of the devices of VN21 decrease from 7 to 3. [6]

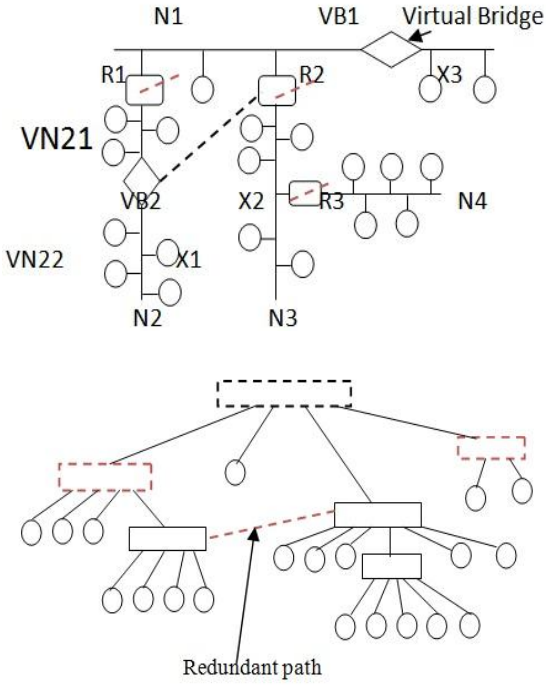

Fig. 3: Virtual bridges

4.2 Linux Kernel

Linux Kernel Version 2.2.16 is the most useful way .It is considered to be immune to most poisoned traffic attacks like teardrop or TARGA. The backlog queue of the system defaults to 128 entries and tcp syn cookies is enabled. After this, the system will be very robust against flood attacks.

4.3 Linux Virtual Server

The load balancer which is used in the Linux Virtual Server (LVS) . LVS inserts itself directly into the kernel and provides a maximum performance again. It stabilizes the system against overload attacks. LVS has two load balancing algorithms: round robin and least connection. By using 'least connection' ,we provide generally a fairer load distribution between the servers.

4.4 DDos Defences

Using filters as shown in Figure 4 to prevent DDos attacks

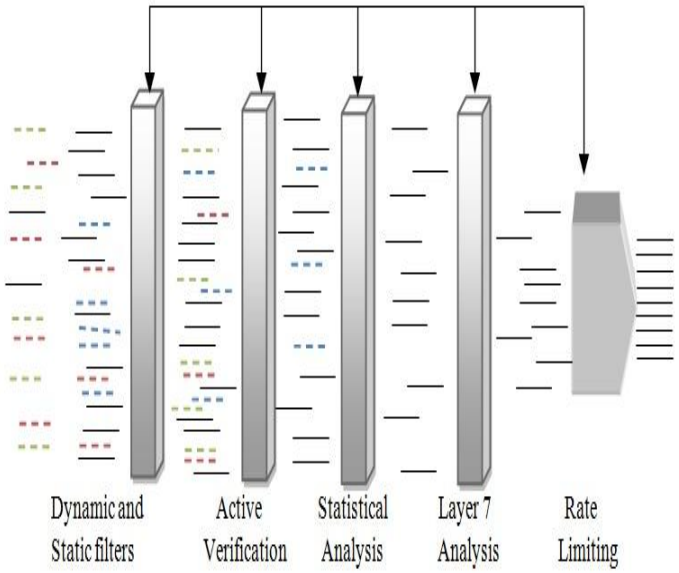

Fig. 4: DDoS Defences

4.5 Countermeasures for some Dos Attacks

Table 2: Attacks, Countermeasure Options and Description.

	Attack	Countermeasure Options	Description
1	Network Level Device	Software updates, packet filtering	By updating software system we will fix some weakness and packet filtering can prevent attacking traffic from entering a network.
2	OS Level	SYN Cookies, drop backlog connections, shorten timeout time	Shortening the backlog time and dropping backlog connections will free up resources. SYN cookies proactively prevent attacks.

3	Applicati. on Level Attacks	Intrusion Detection System	Attack a service or machine by using an application attack to exhaust resources, IDS prevent these attacks
4	Data Flood	Replication and Load Balancing	Extend the volume of content under attack makes it more complicated and harder for attackers to identify services to attack and accomplish complete attacks.
5	Protocol Feature Attacks	Extend protocols to support security.	Trace source /destination packets by a means other than the IP address (blocks against IP address spoofing) and a lot of protocols provide authorization and authentication on entering to system

5. PROPOSAL WORK

Dos is a very important problem in automation system. The paper present solutions to protect system which will be discussed to avoid interruptions in AS and decrease the risk factor.

5.1 Using Trusted Authentication Device

5.1.1 Trusted authentication device (TAD) should be found in AS to manage connecting between users and servers.

Users and server need to be registered in the TAD, only the registered users can connect to the system. Each server has all users signatures in access control list stored on it.

1- System Initialization
When system initialize, TA choose a set of parameters TA signature F and public key d and private key Q = F*d and hash function Z.
2- Registration of the user i
When user i is registered, it will send Ci (User signature) in the registration request,
It will get a set of parameters from TA including d, Ni (user private key), Qi (user public key), Z and Xi Where Xi= E (Ci*F, Ni)
3- Registration of Server j When server j is registered, it will send Sj (server signature) in the registration request, it will get a set of Parameters from the TA including d, Nj (Server private key), Qj (Server public key), Z and Xj Where Xj= E (Sj*F, Nj)

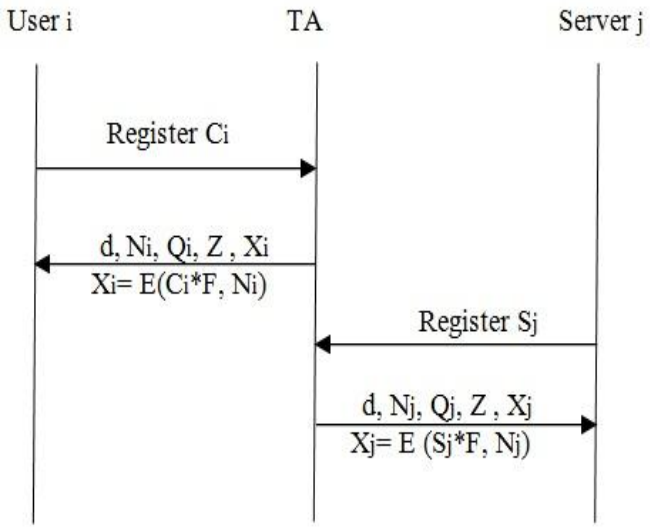

Fig. 5: The Registration of user I and server j

4- Key agreement

- User I generates a random number Mi and sends (Ci, Qi, d, Mi and Ri) to server j

Where Ri = E (Mi*F, Qi).

- After server j receiving the message, it wills ensuring the signature of user i and TA match to the signature which stored on it (for user) and received in registration (for TA).
  Ri = E (Mi*F, Qi) then F= D (Ri ,Qi)/ Mi
  If the signatures matched Server sends to user i the following parameters (Sj ,d ,Qj and Rj)
  Where Rj = E(F, d)
- After user I receives message
  F= D (Rj, d)
  User I ensuring the signature of TA match to the signature which received from server j.
- If the two signatures matched user i start to sending messages to server.

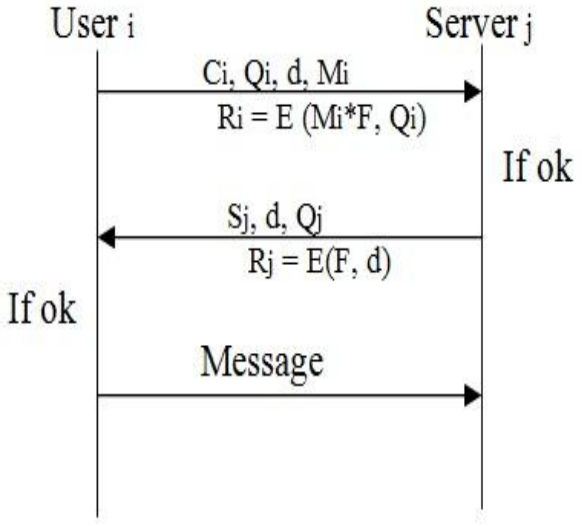

Fig. 6: Key agreement between user i and server j

5.1.2 Trusted authentication device (TAD) should be found in AS to manage connecting between users and servers.

Users and server need to register in the TAD. Only the registered users can connect to the system. Server has all users signatures in an access control list stored on it.

1- when system initialize, TAD generate a set of parameters like TAD private key (Q), TAD public key (L) , hash function , encryption algorithm (AES) and private code for any device which send request to register on TAD (Cj).

2- When user 1 is registered, TAD sends to user Q1, L1, C1, H and encrypted them by AES algorithm.

3- When server is registered, TAD sends to user Q1, L1, C2, H and encrypted them by AES algorithm.

4-After this TAD updates Q.

5- User1 decrypted the message which received from TAD and send to server Q1, L1, S1 and hash code for Q1, L1and S1, encrypted them by AES.

6-Server decrypted the message which received from user1 and compare Q1, L1 with the values which received from TAD and check S1 in access control list, if all values received from user1 equal value on server, it will send to user1 approved message.

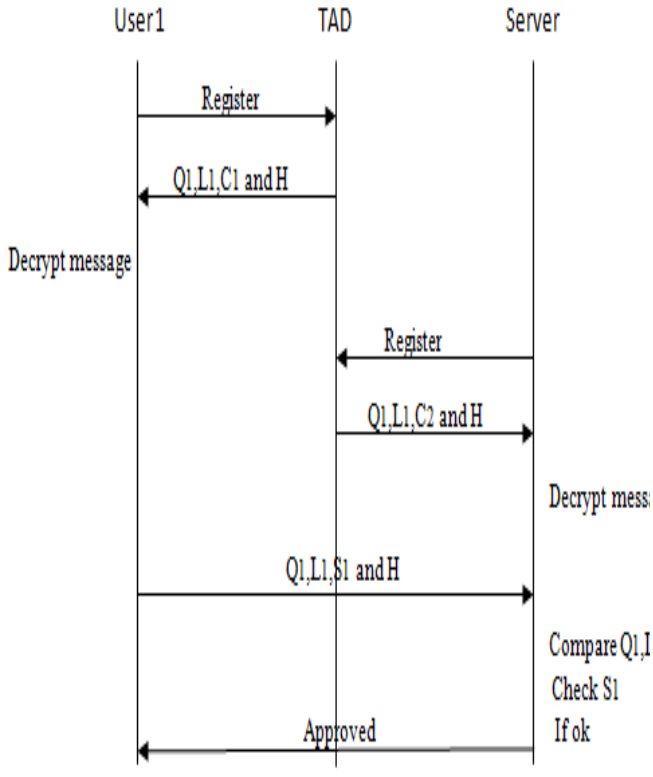

Fig. 7: Trusted authentication device

5.2 Using Counter

It is based on the encrypted communication between two devices by using a counter to protect the transmission against replay attacks. Both the sender (S) and the receiver (R) initiate their counters with the same value G1. Then S sends an encrypted message which contains the message itself and the counter G1, R receives the message and decrypts it. After it has been decrypted, R compares the received counter values with the current valid one. If they are identical, the message is a valid. Now, both S and R increase their counters.

During the transmission of this message, an attacker intercepts it. Later on, the attacker replies this message. Again, R receives the message and decrypts it. Now, the received counter and the current valid one are not identical. And so, R has detected this replayed message and R will discard the message.

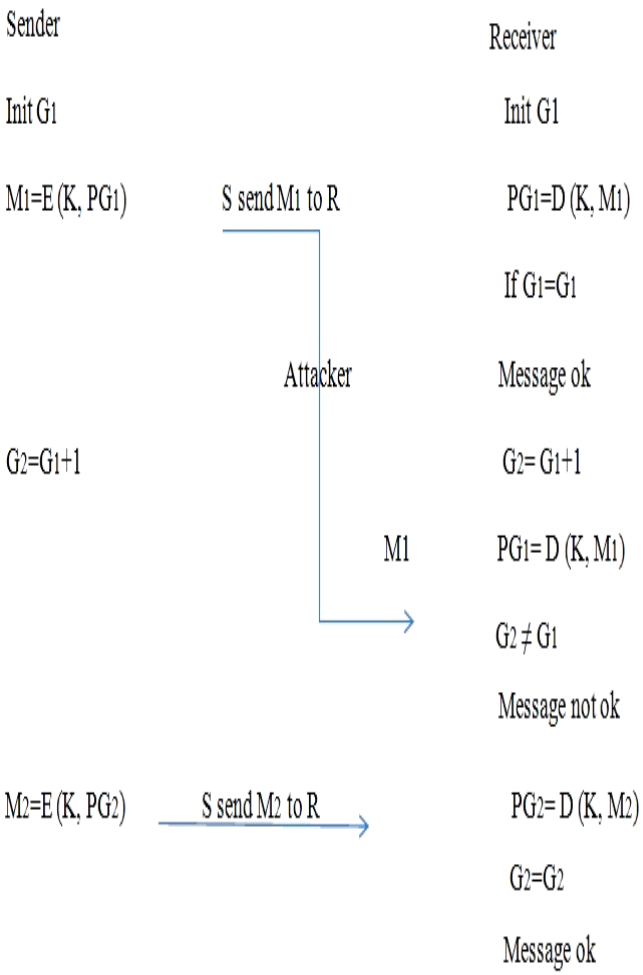

Fig. 8: Counter

5.3 Connecting the Network with Two Routers the First Router is the Basic and the Other Router is Reserve.

The idea is connecting the network with two routers. The first router is the basic and the other router is reserve when any problem happen in the basic router, the system will activate the port to which the network is connected in a spare router. If IDS find attacks from the basic router or if a basic router doesn't send any data to the system for period, a system will deactivate the port in a basic router and activate the port in a spare router. But if a number of devices can connect with a router and connect the half of this number in each network, addresses must not be repeated in the two networks. This solution will decrease the risk factor and connect a number of devices in a network together.

Ex. As shown in Figure 9 connected N1 with port in R1 basic and with R2 spare, if any DoS attack happen in R1 AS. will

deactivate R1 and activate R2. In this case the risk factor will be decreased to zero and the same will happen between N2, N3.

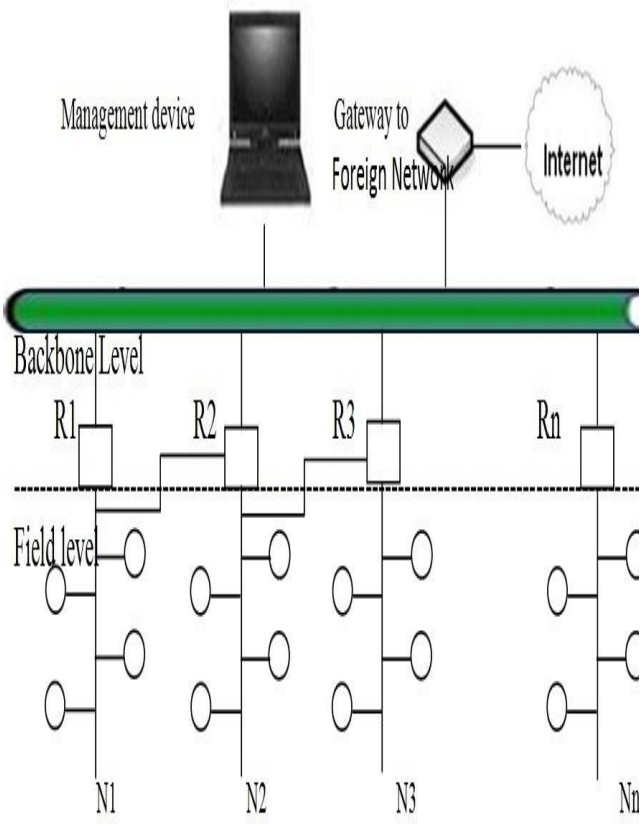

Fig. 9: First router is the basic and the other router reserve

5.4 Dividing the Devices into Normal and VIP Devices and Connecting VIP Devices with Two Networks.

As has a lot of benefits for any building which install on it but benefits would mean different things to different buildings. For industry, energy devices is more important for bank security, in other places server rooms is important etc. in this solution we divide the devices into normal devices and vip devices and connect all devices as shown in figure 10. vip device will connect with two networks if Dos happen in one network system will connect with this device through the other network. This way we will decrease the risk factor in vip devices to zero and in routers, normal devices will decrease risk factor to minimum.

Ex. As shown in Figure 12 A,B,C,D routers and E,F, G vip devices .

By connecting E With A,B routers and consider A basic , B spare when DoS attack or any error happened on A, system will connect to E through B and do the same for F and G devices.

If DoS attack happen on a link which connected between A and a backbone system will connect to A and other devices through E and B and do the same for other networks.

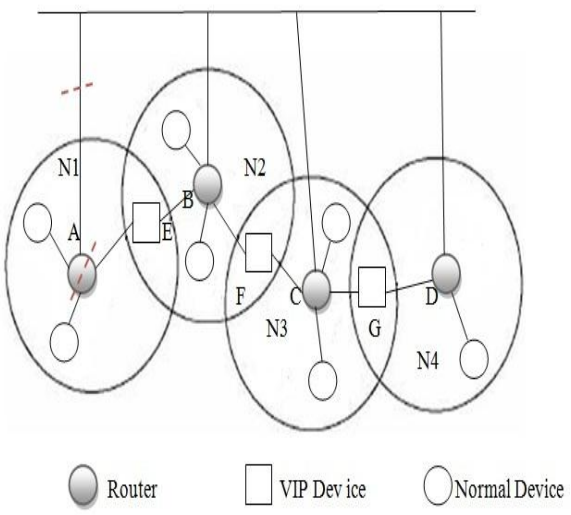

Fig. 10: Connect vip devices

5.5 Trust Point (TP)

5.5.1 Using Trust Point (TP) and Time hours, minutes (T).

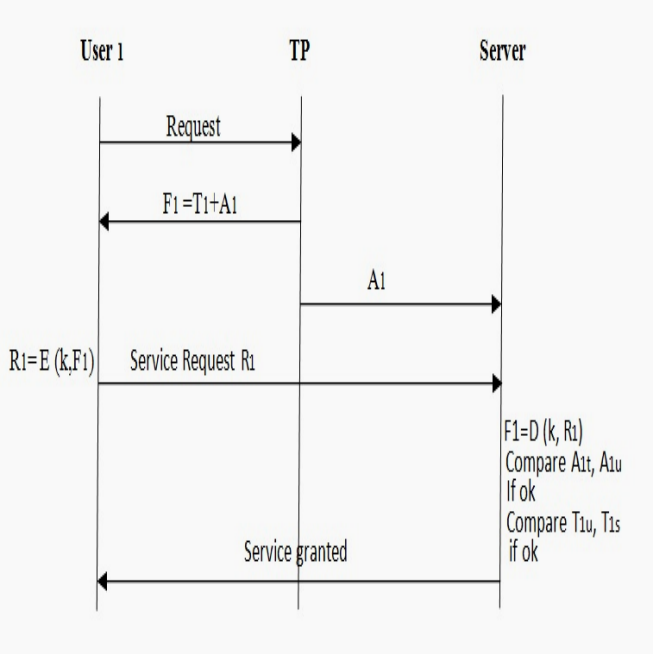

Fig. 11: Trust Point and Time.

1- User 1 send request to Trust point, TP send F1 to user 1 F1= T1+A1 and send A1 to server.

2- User 1 encrypt F1 and send R1 to server R1=E (K, F1).

3- After message reaching to server then server decrypt message

4- F1 =D (K, R1)

5- F1= T1+A1

6- Compare between A1t and A1u if equal, Compare between T1u and T1s if equal, Server send to user service granted.

Note that

- A1t constant reach to server from TP
- A1u constant reach to server from user 1
- T1u time reach from user 1
- T1s time in server

5.5.2 TP in Connecting Between Two Devices.

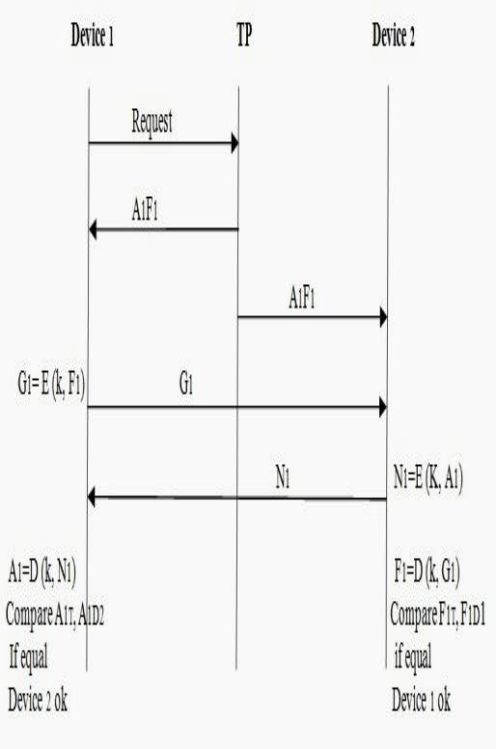

Fig. 12: Trust Point between two devices

1- Device 1 send request to trust point (TP), TP send A1F1 to device1 and device 2.

2- Device 1 encrypt F1 and send G1 to device 2 G1= E (K, F1).

3- Device 2 encrypt A1 and send N1 to device 1 N1=E (K, A1).

4- Device 1 compare A1t, A1D2 if equal device 2 ok.

5- Device 2 compare F1t, F1D1 if equal device 1 ok.

5.6 An Optimal Solution which is Mixing Between the Previous Solutions.

In this solution Ring Topology will be used in connecting routers and devices, connecting vip devices with two networks and using trust point to prevent attackers from access to automation system ; this will decrease risk factor to the minimal.

As shown in figure 13 six networks are connected using ring topology, if an attack happens on normal device in N1 , other devices on network will not affected and risk factor will be 1, if an attack happens on L1, the risk factor will be zero because the two routers will connect to each other through the other routers, the same if an attack happens on any connection between devices or routers like (L2, L3, L4, L5 and L6) the risk factor will be zero. If an attack happens on router like R1, N1 will be connected through vip devices to N6 and connect to the system.

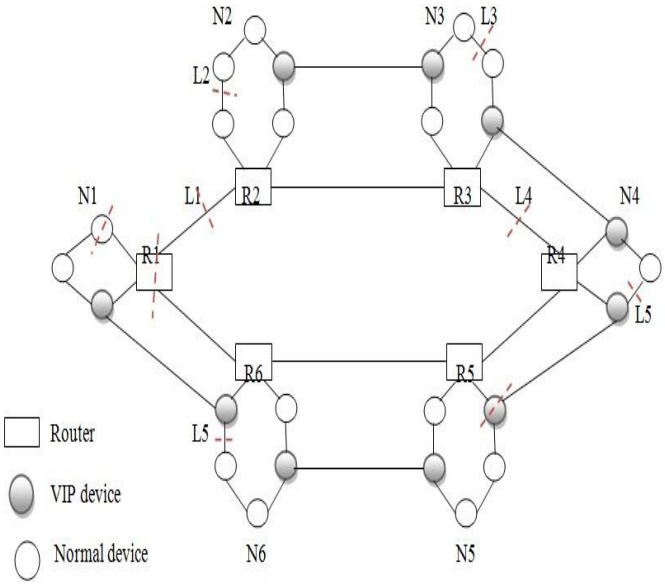

Fig. 13: Ring Topology, connecting vip devices with two networks and using trust point

Table 3: Comparison between Virtual Bridge method, 2 routers method and vip devices method, If network have 7 devices and 2 vip devices

	RF on all devices	RF on vip devices	Notes
Virtual Bridge	4	1 and depend on place of vip devices in network	Number of devices which can connect with router will be decreased to N- VB devices and addresses of VB devices must not be repeated in the two networks.
2 Routers	0	0	Number of devices which can connect with router will be decreased to half and addresses must not be repeated in the two networks.
vip devices	5	0	Number of devices which can connect with router will be N-1 and address of vip devices must not be repeated in the two networks.
Optimal solution	0	0	AS will be more robust against a lot of kinds DoS attacks

RF: Risk Factor
N: Number of devices which can connect to network
VB: Virtual Bridge

6. CONCLUSION AND FUTURE WORK

Protecting automation systems from Dos attacks is a very important task, especially with the rapid growth in the way of attacks and the constant need for more security. Automation system operators are regularly faced with the challenge of extending or upgrading their Security Systems while maintaining a smooth operation method. This paper presented an overview of Dos attacks, detection and countermeasures in automation systems, giving proposed solutions to solve this problem and decrease the risk factor to minimal by: 1- Using Trusted Authentication Device , 2- Using Counter , 3- Connecting the network with two routers; the first router is the basic and the other router is reserve, 4- dividing the devices into normal devices and vip devices, connecting vip devices with two networks, 5- Using trust point to prevent attackers from access to AS. The optimal solution will use the advantages of the previous solutions and IDS is very important in detection methods.

Otherwise, the Dos protection and detection measures must be updated and use a mix of all proposed solutions to achieve the minimal risk factor in AS.

Finally, the expected growth in the denial of service attacks should be offset by significant growth in the protection measures.

7. REFERENCES

[1] Madhuri H. Bhagwat, Amol P. Pande, "Denial of Service Mitigation Method" , Department of Computer Engineering, Datta Meghe College of Engineering, Airoli, Maharashtra, 2013

[2] MEHMUD ABLIZ, "Internet Denial of Service Attacks and Defense Mechanisms" Department of Computer Science, University of Pittsburgh Technical Report, No. TR-11-178, March 2011.

[3] Karimazad, R. and Faraahi, A. an anomaly based method for DDoS attacks detection using rbf neural networks. Proceedings of the International Conference on Network and Electronics Engineering, Singapore, pp. 44–48. IACSIT Press, 2011.

[4] Xiang, Y., Li, K., and Zhou, W. Lowrate DDoS attacks detection and traceback by using new information metrics. IEEE Transactions on Information Forensics and Security, 2011, 6, 426–437.

[5] Loukas, G. and ¨Oke, G. Protection against denial of service attacks: A survey. Comp. J., 53, 2010, 1020–1037.

[6] Wolfgang Granzer, Christian Reinisch, Wolfgang Kastner "Denial-of-Service in Automation Systems" Vienna University of Technology, Automation Systems Group, 1-4244-1506-3/08 2008 IEEE.

[7] Guide to Industrial Control Systems (ICS) Security. NIST SP800-82, 2007. Second Public Review Draft.

[8] Pravin Shinde, Srinivas Guntupalli "Early DoS Attack Detection using Smoothened Time-Series and Wavelet Analysis" CDAC, Mumbai, 0-7695-2876-7/07 2007 IEEE.

[9] Karen Scarfone, Peter Mell "Guide to Intrusion Detection and Prevention Systems (IDPS)" National Institute of Standards and Technology, 2007.

[10] Guide to Industrial Control Systems (ICS) Security. NIST SP800-82, 2007. Second Public Review Draft.

[11] Power System Control and Associated Communications Data and Communication Security. IEC 62351, 2007.

[12] Monowar H. Bhuyan1, H. J. Kashyap1, D. K. Bhattacharyya1 and J. K. Kalita2 "Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions" 2Department of Computer Science, University of Colorado at Colorado Springs, CO 80933-7150, USA.

[13] Josep L. Berral, Nicolas Poggi, Javier Alonso, Ricard Gavald`a, Jordi Torres, Manish Parashar "Adaptive Distributed Mechanism against Flooding Network Attacks Based on Machine Learning" Computer Architecture Dept., Deptartment of Software, Technical University of Catalonia , Dept. of Electrical and Computer Engineering, Rutgers University.

[14] Frank Kargl, Joern Maier, Michael Weber "Protecting Web Servers from Distributed Denial of Service Attacks" Department of Multimedia Computing, University of Ulm, Germany, May 1-5, 2001, Hong Kong. ACM 1-58113-348-0/01/0005.