International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 02 | Feb-2016 www.irjet.net p-ISSN: 2395-0072

Introducing Restricted Access Protocol To Enhance The Security And Eliminate Ddos Attack

Indu Sarmal[1], Sharanjit Singh[2], Amardeep Singh[3]

[1] *Department of CSE, GNDU Regional Campus Gurdaspur, Punjab, India*
[2] *Department of CSE, GNDU Regional Campus Gurdaspur, Punjab, India*
[3]*Department of CSE, GNDU Regional Campus Gurdaspur, Punjab, India*

Abstract – ***The manet is the technique which is used in order to transfer the data among the nodes present remotely as well as at lesser distance from the source. The technique which is used will enhance the communication among the nodes. With the advancement in the technology problems also starts to appear. These problems appear in terms of the attacks. There are number of attacks which are possible when data is being transmitted. One of the common attacks is DDOS. The DDOS attack will jam the traffic and will cause the deadlock in the system. The proposed system will first of all perform the encryption and then transmit the data forward. The data then will be compared against the database of extensions to determine any malicious activity.***

Key Words: *Manet, Traffic, Ddos, Malicious, Extensions*

1. INTRODUCTION

MANET is the mobile Ad-hoc network which is self configuring system in which mobile devices are connected without wires. Each device which is present in the MANET is free to move in any direction. The traffic which is unrelated to the current node must be forwarded to the other nodes present on the network. These nodes may be connected to the organization or it may be connected over the internet. Internet will be used only if distance is larger. MANET has large number of sensors associated with it. The sensors will detect the path and direct the traffic from source to the destination. Data Monitoring and Mining is the common application of the MANET. The MANET is exposed to very huge and large number of users. The intension of the users may be uncertain. So MANET is prone to attacks. There could be large number of attacks which can take place over the MANET. Mainly there is one Common attack and that will be DDOS. DDOS(Distributed Daniel of Service Attack) will target a single system. The system is infected by the Trojen. The system will then transmit large number of packets towards the network. This will cause the network bandwidth to be used heavily. Hence the traffic will be jammed and deadlock will occur over the network. There exist necessary conditions for the deadlock. All the necessary conditions if satisfied simultaneously then deadlock over the network will occur. The necessary conditions will involve No Preemption, Hold and Wait, Circular Wait and Mutual Exclusion. All these conditions are satisfied through DDOS in order for the deadlock to occur within the system. When DDOS attack takes place then zombies are formulated. These zombies are the processes which does terminates however still remain in the memory. These zombies are removed if DDOS handling mechanisms are used.

2. VARIOUS TYPES OF ATTACKS

The attacks on MANET are common all of these attacks are describe through the following table.

Table -1: Name of the Table

Various Attacks External As Well As Internal					
Passive attacks			***Active attacks***		
Eaves-drop ping attacks, traffic analysis and monitoring	Mac layer	Net-Work layer	Trans-port layer	Appli-Cation layer	Other attack
	Jam-ming	Worm-hole, Black-hole, IP spoofing, Modifi cations	Session Hijac-king,Syn Flooding	Data Corru-ption	DOS, DDOS Flood-ing, Gray Hole

All of these attacks will corrupt the data present within the MANET nodes. So some sort of prevention mechanisms is

required. In the proposed system we will suggest a mechanism to overcome the DDOS attack.

3. EXISTING WORK

Large amount of work is done in the area of MANET security. Some of the work which we have analyzed is in the area of Attacks that takes place in case of MANET. [1] Various routing protocols are considered in analyzed work. The rules and regulations are suggested which must be followed in order to ensure that data is transmitted correctly towards the destination. [2] the work is also being done in the area of determining the various attacks on the MANET. The prevention mechanism are also suggested in the existing work.[3] it is not easy to accomplish security within MANET. Security challenges and how we achieve security is suggested in the existing work. [4] the routing protocols are considered and their performance is compared with each other. Performance comparison will be done in the existing work. The performance comparison will be given in terms of a chart which is easy to understand. [5] the MANET in recent years has become popular. Lots of work has been done in this area. Routing strategies are considered in this case. This is one of the most difficult aspects of MANET. [6] due to vulnerabilities in the MANET, large number of security threats which are available. Security threats and solutions are suggested. Security mechanisms if followed successfully data can be secured. [7] Data will be exchanged between the nodes present within the MANET. Lack of infrastructure can cause deception. Trust is difficult to be established due to this problem.[8] there are number of routing protocols which are suggested. Routing is important concept which is discussed in this case. Various types of routing algorithms such as Hybrid , reactive and proactive routing algorithms are considered in the existing work. [9] Network Security mechanisms such as cryptography is also considered. The data which is transmitted first of all encrypted and then transferred. At the receiver ends the data is decrypted. There are very numbers of vulnerabilities that exist within the MANET because of which security threats are imposed. There identification is compulsory which is suggested in the analyzed work. In all the papers we have analyzed security threats and there solutions are suggested. But the concept of insider attack is not indicated. In the proposed scheme the restricted access protocol is suggested. This protocol will go to detect the intruder through questionnaires.

4. DATABASE OF EXTENSIONS

The database is maintained which will contain information about all the extensions which are not understood by the receiving node. The extension which is malicious will cause DDOS attack. In order to prevent that the incoming packet extension will be compared against the database of extension($\sum d_i$). If match occurs then data will not be transferred forwarded. This will detect the attack. The procedure of encryption of data will be performed after the extensions have been checked correctly. Hence extra security feature is introduced in this case.

If $\sum d_i = \sum p_i$ then
Malicious=1
Else
Malicious=0
End of if

5. ENCRYPTION

Encryption is the mechanism by which message is converted into the form which may not be understood by the hackers or malicious users. The encryption strategies are large in number. We will follow RSA technique for the encryption purpose. We have both public as well as private key encryption mechanism available to be used. In public key encryption source as well as destination both knows about the key. But in private key encryption key is hidden. In RSA algorithm both public as well as private keys are used for encoding and decoding purpose. The RSA algorithm will be as described below.

- Two large numbers are chosen which are denoted as p and q
- Determine $n = pq$
  - n is the remainder or modulus for the public and the private keys
- Determine quotient: $\phi(n) = (p-1)(q-1)$.
- Select a value which is of Integer e such that $1 < e < \phi(n)$, and e is co-prime to $\phi(n)$ **ie:** e and $\phi(n)$ share no factors other than 1; gcd(e,$\phi(n)$) = 1.
  - e is the public key exponent
- Compute d which satisfy the Relation $de \equiv 1 \pmod{\phi(n)}$ **ie:** $de = 1 + k\phi(n)$ for some integer k.
  - d will represent the private key exponent.

6. RESTRICTED ACCESS PROTOCOL

In this protocol features of Encryption and restricted extensions will be used. If the data is not malicious then its extension will not match with the database of extensions. Once approved the encryption process will be used to enhance the security mechanisms. The DDOS attack will be prevented since malicious data cannot be repeated and hence blocked by the use of above said protocol. The DDOS attack is shown through the diagram given below. The RAP is efficient in order to prevent this type of attack.

Features of encryption as well as malicious extension checking are used in the proposed model.

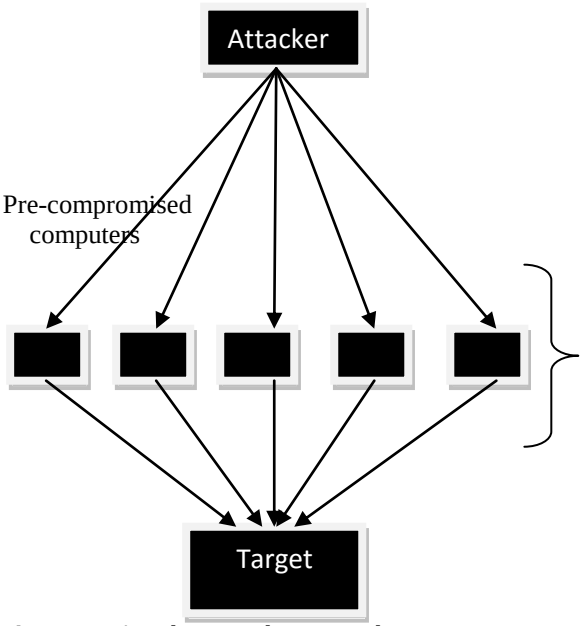

Diagram -1: Ddos attack on a node

7. CONCLUSIONS

The existing system uses the algorithms only to detect the attacks which are generated from outside. This means stress in given only to the external attacks. In the proposed system insider attack is handled with the help of RAP. The restricted access protocol will uses the Encryption as well as database of extension. It will contain the predefined answers from the users of the MANET. The given answers will be compared against the predefined answers. The experiment result indicates that the security is increased by 80% by the use of this protocol.

REFERENCES

[1] A. Shrivastava and A. Shanmogavel, "*Overview of routing protocols in MANET's and enhancements in reactive protocols*," *... Comput. Sci. ...*, 2005.

[2] J. G. Ponsam and R. Srinivasan, "A Survey on MANET Security Challenges,, Attacks and its Countermeasures," *Int. J. Emerg. Trends Technol. Comput. Sci.*, vol. 3, no. 1, pp. 274–279, 2014.

[3] A. Dorri and S. R. Kamel, "Security Challenges in Mobile Ad Hoc Networks: A Survey," *Int. J. Comput. Sci. Eng. Surv.*, vol. 6, no. 1, pp. 15–29, 2015.

[4] H. Paul and P. Das, "Performance Evaluation of MANET Routing Protocols," *Int. J. Comput. Sci. Issues*, vol. 9, no. 4, pp. 449–456, 2012.

[5] D. S. S. D. A. P. Dr.S.S.Dhenakaran, "An Overview of Routing Protocols in Mobile Ad-Hoc Network," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 3, no. 2, pp. 251 – 259, 2013.

[6] W. Li and A. Joshi, "Security Issues in Mobile Ad Hoc Networks-A Survey," *Dep. Comput. Sci. Electr. ...*, pp. 1–23, 2008.

[7] H. Zhao, "Security in Ad Hoc Networks," *Security*, pp. 756–775, 2003.

[8] H. Kaur, V. Sahni, and M. Bala, "A Survey of Reactive, Proactive and Hybrid Routing Protocols in MANET: A Review," *Network*, vol. 4, no. 3, pp. 498–500, 2013.

[9] T. Mamatha, "Network Security for MANETS," no. 2, pp. 65–68, 2012.