ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 8, Issue, 05, pp.32142-32145, May, 2016

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

USING RESTRICTED ACCESS PROTOCOL IN ORDER TO ENHANCE SECURITY AND CONSERVE ENERGY WITHIN MANET

***Indu Sarmal, Sharanjit Singh, Amardeep Singh and Alka**

Department of CSE, GNDU, Punjab, India

ARTICLE INFO

Article History:
Received 28th February, 2016
Received in revised form
23rd March, 2016
Accepted 04th April, 2016
Published online 31st May, 2016

Key words:

Wireless Sensor Network,
MANET, Security,
Malicious.

ABSTRACT

WSN is the networking mechanism through which data is transmitted from source to the destination. The main advantage of the WSN is least utilization of wires causing it to be used by wide variety of users. Security of the WSN will always be at stake because of the extravagant use of the WSN. There is a field of the WSN which is most commonly used known as MANET which is prone to security threats also. In the proposed paper we will consider the security concerns of the MANET and propose solution to the challenges present within the MANET. MANET is diligent in nature hence supporting work of distinct users with varying intentions. Security mechanisms are required to overcome the problems caused due to the malicious intensions of the users

Citation: Indu Sarmal, Sharanjit Singh, Amardeep Singh and Alka. 2016. "Using restricted access protocol in order to enhance security and conserve energy within manet", *International Journal of Current Research*, 8, (05), 32142-32145.

INTRODUCTION

Today lack of empathy cause the threat to the privacy of data transmitted over the network. Legion of work has been down to ensure that the data can be successfully transmitted over the network but more work is required in order to ensure that the data can be transmitted successfully over the wireless network. Most common type of attack which occurs when data is transmitted over the network is DDOS. The term DDOS means distributed Daniel of service attacks which result in the blockage of the resources causing deadlock in the system. The deadlock will have certain necessary conditions associated with it. All of the conditions if satisfied then only this situation occur. This situation is caused by this DDOS attack. The nodes which are considered in the MANET are mobile in nature and they are connected with the network with the help of wireless connection. The main property of the mobile adhoc network is that MANET does not have any centralized ownership. This property serves as both advantage and disadvantage of the wireless adhoc network like MANET. Lack of centralized ownership will result in the security dilemma. It means anyone having desired resources can participate in the network. So some sort of security mechanism is needed in order to ensure that MANET can work without the intervention of unauthorized users (Kaur, 2013) in case data is transmitted from a particular node to another within the MANET routing protocols are to be followed. The routing protocols which are used can be reactive, proactive and hybrid in nature. When reactive protocol is used then data transmission will takes place depending upon the path and the traffic. In case of proactive protocols only shortest path is considered during transmission of data. In case of hybrid protocols both shortest path as well as traffic will be considered (Mamatha, 2012). when MANET is considered nodes communicate with each other without taking the help of the infrastructure. The Infrastructure is not considered hence there does not exist any control of the centralized system on the MANET. So there could be problems which are present when data is transmitted over the network. The analysis and rectification of the problems present within the MANET will be the objective of the paper. The section 1 describes the work which is already done towards the security aspect of the MANET. Section 2 describes the problem definition. Section 3 describes the proposed system. Section 4 gives the results and section 5 describes conclusion and future work.

****Corresponding author: Indu Sarmal,***
Department of CSE, GNDU, Punjab, India

Related work

The work has been down toward the security aspect of the MANET. The solution to the problems present within the MANET has been proposed. The MANET security issues are

primarily caused by the routing of data from one node to another (Kaur, 2013) the protocols which are considered are reactive, proactive and hybrid in nature. The protocols specified have their own advantages and disadvantages. The hybrid protocol is considered the best among the available protocols. The network security (Mamatha, 2012) is another concerns specified within the MANET. The MANET is used by wide variety of users. Every user will have distinct intensions so it is required to tackle the intensions of the user to preserve the data present over the MANET (Veeraraghavan, 2007). Securing a Wireless Ad Hoc Network is a major concern for researchers.

Due to varied characteristics of Ad Hoc Networks, they are vulnerable to internal as well as external attacks. Many solutions have been proposed and currently being improved upon in this area. Most of these solutions involve encryption; secure routing, key management etc. Each of them is designed to operate in a particular situation, which may fail to work successfully in other scenarios. The present work in this paper offers an alternate to improve the trustworthiness of the neighborhood and secure the routing procedure. It helps in computing the trust in neighbors and selecting the most secure route from the available ones for the data transfer. It also helps detecting the compromised node and virtually it removing from the network (Shrivastava and Shanmogavel, 2005) the enhancement in the routing protocols are consider in this case. The protocol consider for evaluation is reactive in nature. The reactive protocol will be the one in which traffic and shortest path both will be considered. The protocol which is suggested is dynamic in nature (Paul and Das, 2012).

The evaluation of various routing protocols are considered in this case. The protocols can be static and dynamic in nature. The static protocols are cost effective however the dynamic protocols are expensive in nature. The dynamic protocols will consider the traffic and shortest path but the static protocols consider only the shortest path (Dhenakaran, 2013). In recent years mobile ad hoc networks have become very popular and lots of research is being done on different aspects of MANET. Mobile Ad Hoc Networks (MANET)-a system of mobile nodes (laptops, sensors, etc.) interfacing without the assistance of centralized infrastructure (access points, bridges, etc.). There are different aspects which are taken for research like routing, synchronization, power consumption, bandwidth considerations etc. This paper concentrates on routing techniques which is the most challenging issue due to the dynamic topology of ad hoc networks. There are different strategies proposed for efficient routing which claimed to provide improved performance. There are different routing protocols proposed for MANETs which makes it quite difficult to determine which protocol is suitable for different network conditions .This paper provides an overview of different routing protocols proposed in literature and also provides a comparison between them (Ponsam and Srinivasan, 2014). Ad-hoc networks have lots of challenges than traditional networks. It has challenges like infrastructure less and self organizing networks. They don't have any fixed infrastructure. In MANET, there will be no centralized authority to manage the network. Nodes have to rely on other nodes to keep the network connected. As the ad-hoc network is dynamic and every transmission in these networks become vulnerable to many number of attacks and security becomes a major issue. In this survey paper we study the different security attacks to ad-hoc networks and also discussed available solutions. We try to provide a brief introduction to the types of attacks and possible counter measures to prevent the attacks. From the analyzed papers we conclude that the existing protocols are based on the routing protocols but they does analyze the contents of data transmitted and also extensions of the packets are not analyzed. In the proposed paper we will perform the both of the above said operations.

Problem Definition

In the existing system the analysis of the routing protocols are made. The routing protocols suggest that the data transmission can be made much faster using the situational protocols which means protocols will show optimal behavior depending upon the situations in which it is used. Also when malicious user is encountered then nothing is done in order to detect and rectify the problems if any. The main problem present within the existing system is non detection of malicious data present within the file and checking for the security related with the extension of the files being transmitted. In the proposed paper both of the above situations will be handled.

Proposed system

The proposed system will going to handle the latitude of the problem by creating a protocol which is going to handle the transmitted data by analyzing it for accuracy. The proposed model MANET security is listed through two levels. First level will check the contents of the files. Second level will check the extensions. The proposed system will follow the mechanism of two layer security mechanism. In the first layer the contents of transmitted file will be checked and in the second case the extensions of the transmitted file will be checked. In case the malicious node is detected then the threshold value will be incremented by one. If the threshold expires then report will be transmitted to the certification authority. The node will be blocked permanently in this case. The proposed model describes all the nodes present within the network. The nodes can be transmitter or receiver. All other nodes present over the network can be inspecting nodes. Any malicious activity detected by the inspecting node will cause the threshold to be incremented by one. Threshold should not expire in order for the node to be continues in the network. The proposed algorithm will be as follows:

The above said algorithm will transfer the data from source to destination only if the packet transmitted is not malicious and threshold value is less than the prescribed tolerance.

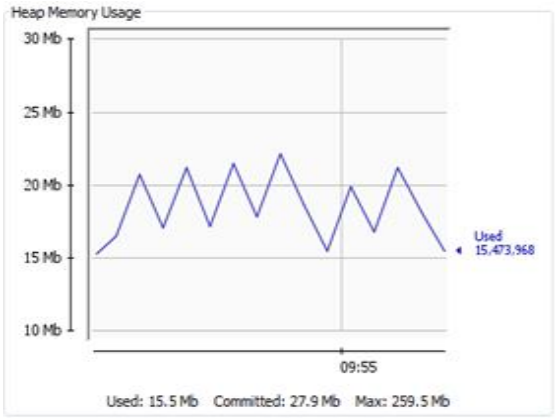
RESULTS

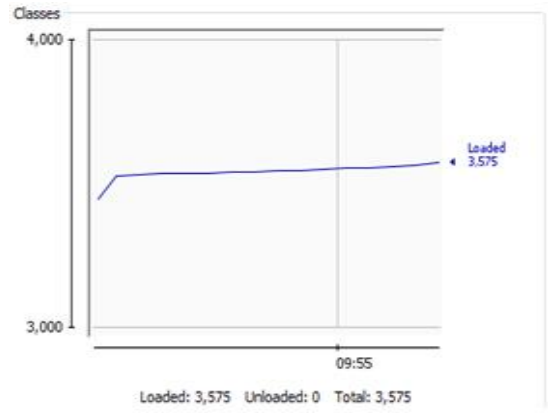
The simulation is tested for random 100 node network. The location of base station was selected at (50,175) in network. The reference network used in simulation has 100 nodes, in a 10×10 square field. Each node has 0.5 J of initial energy. The packet size is 2,000 bits, and 0.05 % of the nodes are selected as cluster heads.

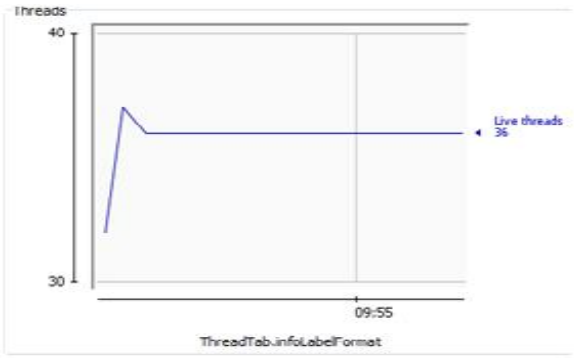
Algorithm Malcious(Packet$_i$,D$_i$)

// Packet is the dictionary containing verified character set and D indicates extension //dataset

a) If(th<PT) then
b) Input the packet sequence(P$_i$)
c) Record the extension of the file(E$_i$)
d) Compare $\sum P_i - \sum Packet_i$
Goto step d
Else
Th=Th+1
I=I+1
Malcious(Packet$_i$,D$_i$)// Move to the next packet in sequence
End of loop
e) Compare $\sum F_i = \sum D_i$
Malicious detected
Ih=Ih+1
Else
Transmit data over MANET
Else
Source Blocked
f) Stop







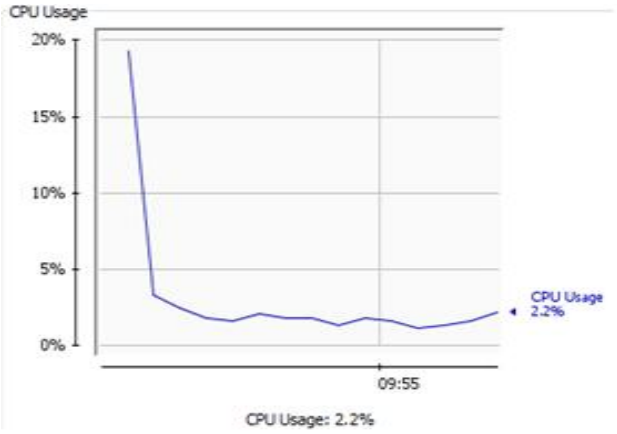


Figure 1. Showing the result in terms of the Memory Usage, CPU Usage and load

When proposed system is used energy consumption is significantly reduced. The result of the proposed and existing system is as describe through the tabular form

Table 1. Showing the difference between the existing and new system in terms of the parameters

Parameters	Existing System	New System
Redundancy	Packets Transfer (200)	Packet Transfer(155)
Power Dissipation	5 W	3 W
Bandwidth Utilization	20	15
Duty Cycle	15	33.33
Security	Encryption	Extension Based Security
Packet Loss	High	Low

The result indicates that the proposed algorithm will consume much less energy than the existing algorithm.

Conclusion and future work

The proposed algorithm will enhance the security process present within the MANET. The results indicate that the proposed algorithm will consume much less energy as compared to the existing algorithm. The proposed algorithm utilizes two levels of security which will enhance the overall process of authentication which is missing in the existing approach. There could still be security enhancement which can be suggested. These modifications include introducing random key in the existing approach to enhance the security.

REFERENCES

Ali, M. A. 2011. "*Security Issues regarding MANET (Mobile Ad Hoc Networks): Challenges and Solutions*," no. March, 2011.

D. S. S. D. A. P. Dr.S.S.Dhenakaran, 2013. "*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.

Djenouri, D. and Khelladi, L. 2005. "*A survey of security issues in mobile ad hoc networks*," *IEEE Commun. Surv.*, vol. 11, no. 02, pp. 129–137.

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

Fasanghari, M. and Montazer, G. A. 2010. *"Design and implementation of fuzzy expert system for Tehran Stock Exchange portfolio recommendation,"* *Expert Syst. Appl.*, vol. 37, no. 9, pp. 6138–6147.

Gagandeep, Aashima, and P. Kumar, 2012. *"Analysis of different security attacks in MANETs on protocol stack a-review,"* *Int. J. Eng. Adv. Technol.*, vol. 1, no. 5, pp. 269–275.

Garg, N. 2009. *"MANET Security Issues,"* *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 9, no. 8, pp. 241–246.

Gupta, A. K., Sadawarti, H. and A. K. Verma, 2011. *"Review of Various Routing Protocols for MANETs,"* *Int. J. Inf. Electron. Eng.*, vol. 1, no. 3, pp. 251–259.

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

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

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

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

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

Rai, P. and S. Singh, 2010. *"A Review of ' MANET ' s Security Aspects and Challenges ',"* *IJCA Spec. Issue "Mobile Ad-Hoc Network", MANETs*, pp. 162–166.

Shrivastava, A. and Shanmogavel, A. 2005. *"Overview of Routing Protocols in MANET's and Enhancements in Reactive Protocols,"* *… Comput. Sci. ….*

Ulnerabilities, V. and Chou, T. 2013. *"S Ecurity T Hreats on C Loud C Omputing,"* vol. 5, no. 3, pp. 79–88.

Veeraraghavan, P. and V. Limaye, 2007. *"Security Threats in Mobile Ad Hoc Networks,"* *2007 IEEE Int. Conf. Telecommun. Malaysia Int. Conf. Commun.*, vol. 1, pp. 1–22.

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

****