iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VIII **Month of publication:** August 2017

DOI: http://doi.org/10.22214/ijraset.2017.8122

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

Securing Mobile and Ad Hoc Network against Packet Dropping Attack

Pinki[1], Sonal[2]
M.Tech Student[1], Assistant Professor[2], BPS Mahila Vishwavidyalaya Khanpur Kalan (Sonipat)

***Abstract:** Ad hoc networks had been considered as wireless networking paradigm for mobile hosts for particular purpose only. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep network connected. In today's society with development of mobile devices this had become important to stay online all time. In order to stay online all time this must be possible to set up a network fast & cost effective when moving between different infrastructures, ad hoc networks deals with this kinds of issues. Then we discuss security criteria of mobile ad hoc network & present main attack types that exist within it. After ad hoc network had been established nodes that connect network might move, that one military squad is under heavy attack & had to escape. In ad hoc networks would be competent to move to all commerce.*

***Key Words:** Ad Hoc Network, Security, Intrusion Detection, Secure Routing*

I. INTRODUCTION

An ad hoc network is a network that is composed of individual devices communicating with each other directly. Many ad hoc networks are local area networks where computers or other devices are enabled to send data directly to one another rather than going through a centralized access point. Ad hoc network does not need any router. It does not need any wireless base station this network is established for single session only. If someone wants to share file in multiple computers then he could set more than one hop ad hoc network that can be used to transfer information on more than one node. It is created to solve specific problem. It becomes permanent network if someone is going to establish such network for longer period.

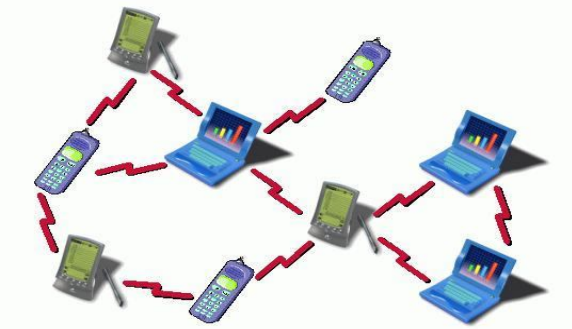


Fig 1. Mobile ad hoc network

The primary challenge in building a MANET is equipping each device to continuously maintain information required to properly route traffic. Such networks might operate by themselves or might be connected to larger Internet.
They might include one or several & different transceivers among nodes. This outcome in a highly dynamic, autonomous topology. Research on Wireless AdNetworks had ongoing for decades. Ad hoc network has played a main role by in military supplications &linked research efforts, for example, global mobile information systems (GloMo) program & near-term digital radio (NTDR) program. Current years have see a fresh spate of trade & commercial applications for wireless ad hoc networks[2], as viable communication[5] equipment & portable computers become more compact & available.

A. Advantages of MANETs

The following are advantages of MANETs:

1) Independence from central network administration
2) Self-configuring, nodes are also routers

3) Self-healing through continuous re-configuration
4) Scalable: accommodates addition of more nodes

B. Disadvantages of MANETs

Some of disadvantages of MANETs are as follows:
1) Limited resources & physical security.
2) Intrinsic mutual trust vulnerable to attacks.
3) Lack of authorization facilities.
4) Volatile network topology makes it hard to detect malicious nodes.
5) Security protocols for wired networks cannot work for ad hoc networks

II. COMMUNICATION MECHANISM

The endpoint with in an inter process communication is called a socket, or a network socket for disambiguation. Since on the whole communication among computers Internet is based on Protocol, an almost equivalent term is Internet socket. Data transmission between two sockets is organized by communications protocols [6], usually implemented within operating system of participating computers.

A. Client Server Model

It is possible for two network applications to begin simultaneously, but this is impractical to require it. Therefore, this makes sense to design communicating network [8] applications to perform complementary network operations with in sequence, rather than simultaneously.

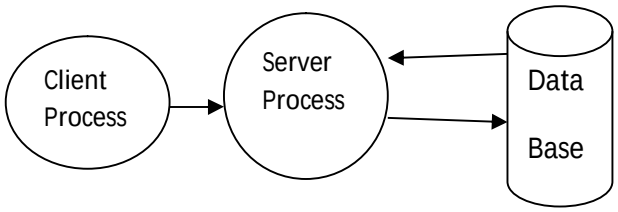


Fig 2. Client server model

Port	Service Name, Alias	Description
1	Tcpmux	TCP port service multiplexer
7	Echo	Echo server
9	Discard	Like/dev/nu11
13	Daytime	Systemsdate/time
20	ftp-data	FTP data port
21	ftp	Main FTP conection
23	telnet	Telnet connection
25	Smtp, mail	UNIX mail
37	Time, timeserver	TIME server
42	Name server	Time server
70	Gopher	Text/menu information
79	Finger	Current users
80	www,http	Web server

Table 1: Port

Above table represent the port no and the protocol used in case of different servers such as echo server, time server, UNIX server, web server.

B. Data Flooding

Not every successful reading of a tag (an observation) is useful for business purposes. A large amount of data might be generated that is not useful for managing inventory [10] or other applications. For example, a customer moving a product from one shelf to another, or a pallet load of articles that passes several readers while being moved in a warehouse, are events that do not produce data that is meaningful to an inventory control system.

III. EXISTING PROTOCOL

Enhancing network lifetime & increasing packet delivery ratio is strongly targeted in Existing protocol. Former criterion is met by considering Euclidean distance in existing fuzzy system in order to transmit packets to node nearest to destination as well as latter criterion considers number of neighbors of each neighbor node in order to transmit packets to neighbor node which had more neighbors rather than other neighbor nodes.

IV. PROPOSED ALGORITHM

A. At beginning consider Data packet & control packet are packets which are used.
B. Reduce Data Packet by replacing of T_Data with xT_data.
C. Select CNs from among neighbors with (RE>REavg) & (ABS>ABSavg).
D. Specify NP based on sender node, SR & base station.
E. Determine distance between CN & np, Determine number of neighbors at CN.
F. Perform Fuzzification using Fuzzy set, cluster Base, Rule base in inference Engine.

IV. RESULT & DISCUSSION

In our research we would establish a MANET Environment to test flow of packets then we would make develop of packet sender & receiver module. After that we would test transmission, processing, queuing delay in packet transmission. Then we would compare both work previous & proposed work. We would use java based socket programming to transfer packet from sender to receiver in minimum time.

A. Comparative Analysis of Overall Time Consumption in Tradition & Proposed Comparison System

PACKETS	TRADITIONAL	PROPOSED
10	5	2
20	5	2
30	8	3
40	8	3
50	10	4
60	10	4
70	11	5
80	11	5

Table 2: Time consumption in tradition & proposed comparison system

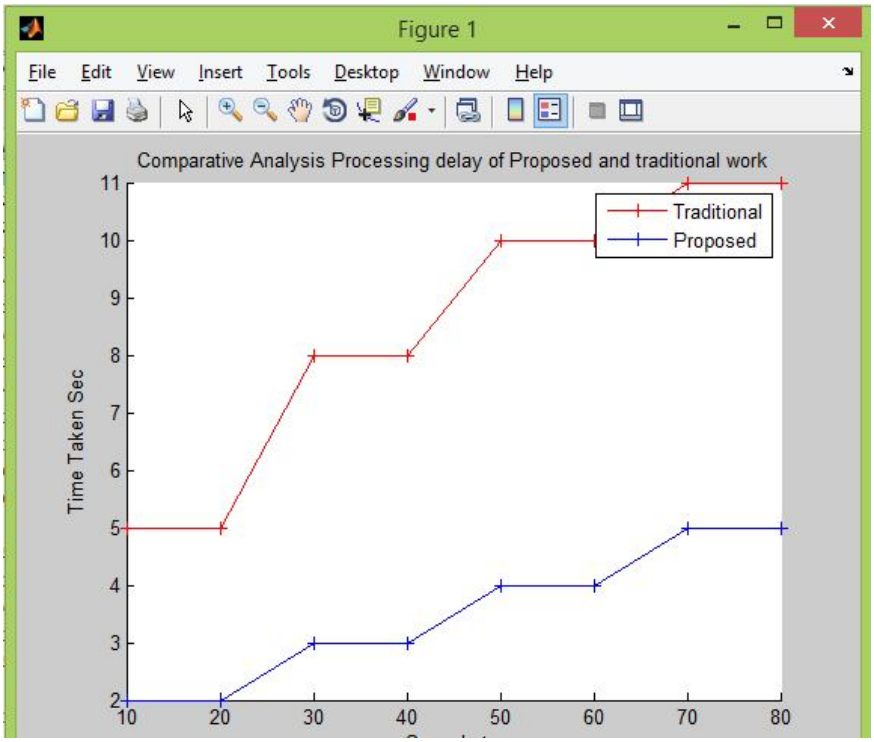


Fig 3.Comparative analysis of overall Time consumption

B. Comparative Analysis of Queuing Delay in Tradition & Proposed Comparison System

FILE SIZE	TRADITIONAL	PROPOSED
10	6	3
20	6	3
30	9	4
40	9	4
50	11	4
60	11	4
70	13	5
80	13	5

Table 3: Queuing delay in tradition & proposed comparison system

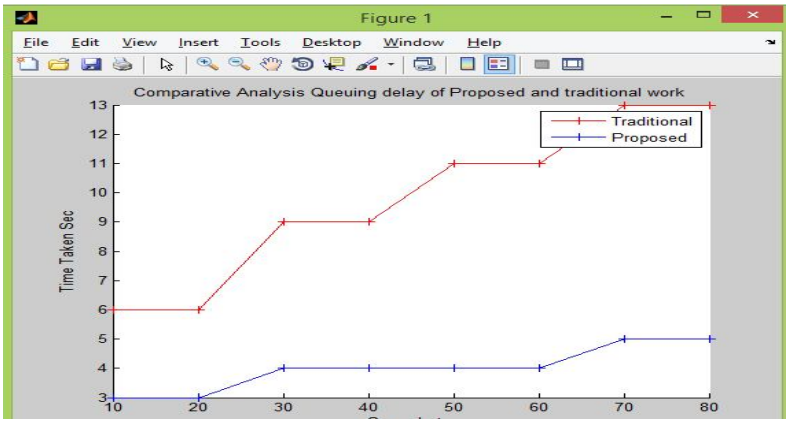


Fig 4. Comparative analysis of Queuing delay in tradition & proposed comparison system

C. Comparative Analysis of File Size in Tradition & Proposed Comparison System

PACKETS	TRADITIONAL	PROPOSED
10	4020	1020
20	8090	2050
30	12100	3600
40	16201	4201
50	20300	5100
60	24200	6300
70	29002	7210
80	33100	8543

Table 4: Comparative analysis of File Size in tradition & proposed comparison system

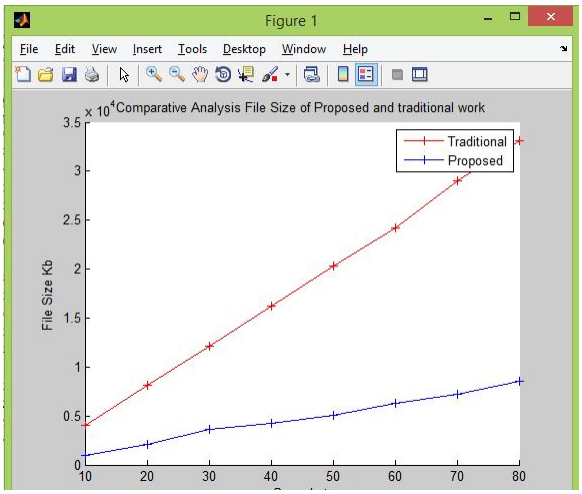


Fig 5. Comparative analysis of File Size in tradition & proposed comparison system

V. CONCLUSION

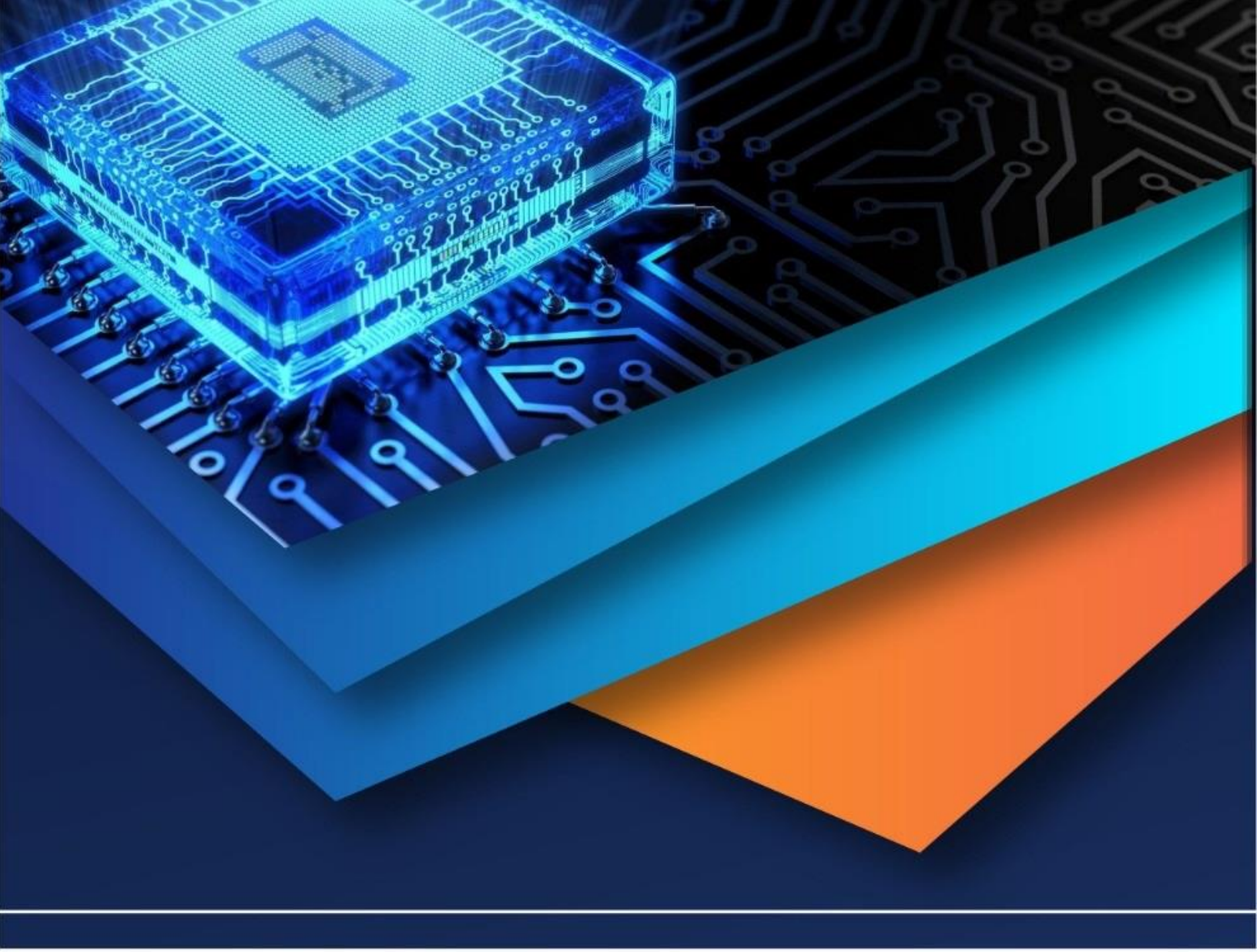
Issue of ADHOC Network security is demand of day. Proposed implementation had enhanced security of ADHOC Network. Data transmission could be made more secure from hacker to by encrypting data on sender side & decrypt it on client side. To perform this we need to merge two technologies. & on part of .net play its best role to develop GUI interface to make system easy to operate by user

A. Socket Programming
B. Data Encryption.

REFERENCES

[1] Agi, I., Gong L, "An empirical study of secure mpeg video transmissions", In: Proceedings of the Symposium on Network and Distributed System Security, pp. 137–144. IEEE Press, New York (1996).
[2] Cheng H., Li, "Partial encryption of compressed images and videos". IEEE Trans. Signal Process.**48** (8), 2439–2451 (2000).
[3] Chiaraluce. F., Ciccarelli. L., Gambi. E., Pierleoni, P. Reginelli, "A new chaotic algorithm for video encryption". IEEE Trans. Consum. Electron.**48**(4), 838–844 (2002)
[4] SudhirAgrawal, Sanjeev Jain, and Sanjeev Sharma, "A survey of routing attacks and security measures in mobile ad-hoc networks", arXiv preprint arXiv:1105.5623, 2011.
[5] Dr. Mazin Sameer Al-Hakeem, "Development of Fast Reliable Secure File Transfer Protocol", Journal of Zhejiang University-SCIENCE , 2013
[6] S Sankara Narayanan and S Radhakrishnan, "Secure aodv to combat black hole attack in manet", In Recent Trends in Information Technology (ICRTIT), 2013 International Conferenceon, pages 447{452. IEEE, 2013.
[7] KishorJyotiSarma, Rupam Sharma, and Rajdeep Das, "A survey of black hole attack detection in manet", In Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014International Conference on, pages 202-205.IEEE, 2014.
[8] Maulik H. Davda(2014), "A Review Paper on Study of Attacks in MANET with Its Detection & Mitigation Schemes",International Journal of Advance Research in Computer Science & Management Studies Volume 2, Issue 4, April 2014

[9] Kshitij Bhargava, "Packet Dropping Attacks In Manet: A SURVEY", Journal of Advanced Computing & Communication Technologies (ISSN: 2347 - 2804) Volume No.2 Issue No. 3, June 2014
[10] Sharad Pratap Singh, "security configuration & performance analysis of ftp server", intelligent Computing, Networking & Informatics Advances in Intelligent Systems & Computing ,2014
[11] Debarati Roy Choudhury, LeenaRagha, and NileshMarathe, "Implementing and improvingthe performance of aodv by receive reply method and securing it from black hole attack",Procedia Computer Science, 45:564{570, 2015.
[12] Sandeep Kumar Suman, "A Survey of Black Hole Detection Techniques in WSNs" , International Journal of Advanced Research in Computer & Communication Engineering, 2015
[13] Arpana Akash Morey1(2015), " Review of a Secure Approach to Prevent Packet Dropping & Message Tampering Attacks on AODV-based MANETs" , International Journal of Computer Science & Information Technologies, Vol. 6 (3) , 2015, 2373-2376
[14] Mohamed Elboukhari (2015), "Impact analysis of black hole attacks on mobile ad hoc networks performance", International Journal of Grid Computing & Applications (IJGCA) Vol.6, No.1/2, June 2015
[15] Lidong Zhou Ali Jalooli, Rafidah MdNoor,Rashid Hafeez Khokhar, Jaime Lloret, "Securing Ad Hoc Networks", Wireless Networks , Springer ,2015
[16] Aaditya Jain, "Advance Trends in Network Security within Honey pot & its Comparative Study within other Techniques" ,December 2015
[17] Aditi, Joy KaranSingh, "Analysis of various Security Attacks in Mobile Adhoc Network", International Research Journal Of Engineering & Technology (IRJET) VOLUME: 03 ISSUE: 07 | JULY-2016 .
[18] Sonu MadhuViswanatham, "Review Paper on Securing Wireless", IEEE 2016
[19] Amit Rathee "Wireless Sensor Network- Challenges & Possibilities", International Journal of Computer Applications (0975 – 8887) Volume 140 – No.2, April 2016
[20] Shantala Devi Patil "Overview of Issues & Challenges in Wireless Sensor Networks", International Journal of Application or Innovation in Engineering & Ma Volume 5, Issue 5, might 2016
[21] Nidhi Suman, "Secure & Energy Efficient Routing in Wireless Sensor Networks: A Review", International Journal of Computer Science & Engineering Technology, Feb 2016.
[22] Mohammad Samadi Gharajeh, Sohrab Khanmohammadi, "DFRTP: Dynamic 3D Fuzzy Routing Based on Traffic Probability in Wireless Sensor Networks".
[23] Sellers, K.F., Morris, D.S., Balakrishnan, "Bivariate Conway–Maxwell– Poisson distribution: formulation, properties, & inference", J. Multivariate Anal., 2016, 150, pp. 152–168
[24] Chowdhury, S.R.; Bari, M.F.; Ahmed, R.; Boutaba, "A low cost network monitoring framework for Software Defined Networks", In Proceedings of 2016 IEEE Network Operations & Management Symposium (NOMS), Krakow, Poland, 5–9 might 2016; pp. 1–9.
[25] Mikhaylov, K.; Petaejaejaervi, .J.; Haenninen, " Analysis of Capacity & Scalability of LoRa Low Power Wide Area Network Technology", In Proceedings of 22th European Wireless Conference on European Wireless, Oulu, Finland, 18–20 might 2016; pp. 1–6.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY