# A Modified Pass Based Identification Technique to Make ZRP Secure

**Er. Namisha**
*M. Tech Student*
*Department of Computer Science Engineering*
*Geeta Institute of Management and Technology, Kurukshetra University, Haryana, India*

**Er. Sahil Batra**
*Assistant Professor*
*Department of Computer Science Engineering*
*Geeta Institute of Management and Technology, Kurukshetra University, Haryana, India*

## Abstract

Mobile Ad Hoc network comes with many advantages and applications in the situation where the time for recovery is very less. These advantages come along with some security risks. The approaches used to form MANET comes under three categories proactive, reactive and hybrid. The proactive and reactive has a vast research linked with them compared to the hybrid. The hybrid approach takes the advantage of both proactive and reactive. The hybrid has the advantage to follow the positives of both. In this paper, the implementation of a modified pass based identification and authorization technique is done over the hybrid protocol ZRP and analysis compared to the traditional available approach for ZRP is presented. The implementation focuses on the secure message transmission along with the authentication of nodes on the network. It differs from the message encryption techniques as the authentication of the node is also done in the process.

**Keywords: ZRP, Security, Authentication, Hybrid, MANET, Identification.**

## I. INTRODUCTION

In this new age of communication, the advent of mobile computing has revolutionized our information society. Routing is the act of moving information from a source to a destination on a internetwork.During this process is at least an intermediate node within the internal network. Routing concept basically involves two activities: first, determination of optimal routing paths and secondly, transfer of the groups of information (called packet) through an internetwork. Routing protocols use various indicators to calculate the best route to route packets to their destination. For communication purpose in MANETs, nodes need to identify other nodes of their interest. Therfore, mobile nodes can be identified by their own identity of spatial and temporal invariance. For example, nodes propose their identity when joining MANET's network. Nodes should be assisted with additional security procedures to ensure the confidentiality, integrity, and authenticity of their information exchange with interested nodes. In case of any certification Authority (C A) or any preexisting communication and security infrastructures, nodes may have to deal with unknown relaying nodes without the information about them. To overcome this weakness, a identity-based pass management and authentication is used. To make ZRP secure and more robust to attacks in MANETs, the modifications are done in the ZRP which is available till date.

## II. RELATED WORK

Raj Shree Sanjay Kr. Dwivedi, Ravi Prakash Panday (2011) will document "design improvements in ultiple detection ZRP Black Hole nodes mobile ad hoc networks" considered an area with several black hole nodes that can work in collaboration and we are implementing the Secure-ZRP protocol that can be used to prevent black hole attacks in MANET. They evaluated the performance in the simulator QualNet. Their analysis indicates that S-ZRP is a very suitable and efficient protocol to stop this attack.

Jonny Karlsson, Laurence S. Dooley and Goran Pulkkis (2012) in their paper entitled "Safety routing in mobile ad hoc networks" presented a review of MANET routing protocols is briefly presented. MANET Security Attacks against routing can be and passive or active. The aim of the former is the search for information, monitoring of network traffic instance, while the second is performed by malicious nodes with the express intent to annoy, modify or discontinue MANET routing. An overview of active attacks based on modifying, impersonation / spoofing, manufacturing, wormhole, and selfish behavior is presented. The importance of cryptography and confidence in the MANET routing is secure also described, with relevant security extensions to existing routing protocols described and evaluated MANET. A comparison of existing secure routing protocols form the main contribution in this paper, while some future research challenges in the routing MANET secure are discussed.

Ionut Constantin Mihai Luca Pura (2013) in their paper entitled "Securing ZRP - a hybrid Ad Hoc Routing Protocol" has considered scenarios in which the network is very large and the characteristics of communication are not the same everywhere but may be clustered. The best type of ad hoc routing protocols in this case would be a hybrid. From the point of view of security, research had addressed proactive ad hoc and reactive routing protocols, but very little of those hybrids. Their purpose

All rights reserved by *www.ijste.org*

was to investigate how such a protocol can be fixed. For this, they chose a very popular hybrid protocol routing, namely ZRP. From an implementation of this protocol NS2, we obtained using asymmetric cryptography. Their new implementation provides authentication, confidentiality and non-repudiation for all messages sent via the protocol for routing information and data as well.

Shah Chaitas, Professor Manoj Patel (2014) will document entitled "Improving ZRP protocol against Blackhole Attack" provides information on the different types of routing protocols that have been discovered. These protocols can be classified into three main reagents categories (on request) Ad-hoc On Routing Protocol Demand (AODV), proactive (table-driven) OLSR and Hybrid Routing Area protocol routing protocol (ZRP). Thus mobile network AdHoc for routing protocols must face the challenge of power transmission frequently insufficient, asymmetric links and change the topology. Both proactive and reactive routing protocols be ineffective certain circumstances. The hybrid protocol Routing Protocol Zone (the ZRP) combines the benefits of proactive and reactive approaches and maintains a topology map making day of an area centered about each network node. Within the area, routes are immediately available for the packet transmission. Thus, for destinations outside the zone, Zone Routing Protocol uses a route discovery procedure, which benefits the local routing information areas. However, because of security vulnerabilities of routing protocols and unprotected wireless networks remains to attacks by malicious different nodes.

## III. PROPOSED ALGORITHM

### *A. Problem Description:*

Security is a vital factor in MANET because of its sensitive applications. However, the characteristics of MANET pose challenges and opportunities in achieving safety objectives to ensure confidentiality, authentication, integrity, availability, access control, and non-repudiation. The purpose of confidentiality is to keep the transmitted information unreadable to unauthorized users or nodes. The purpose of authentication is to ensure a communicating entity is in communication with another legitimate entity. Without authentication an attacker can impersonate an authenticated node and thus take control of the entire network. The purpose of integrity is to be able to keep the sent message to be altered or destroyed in the transmission illegally. When data is sent over the wireless medium, the data can be modified or deleted by malicious attackers. The purpose of non-repudiation is linked to a fact that if an entity sends a message, the entity cannot deny that the message was sent by him. By producing a signature for the message, the entity cannot deny later the message.

### *B. Design Considerations:*

1) Attacks such as Jamming is not possible in the network i.e network is able to hadle the computational load. the network links are either unidirectional or bidirectional; that is, if node A is able to transmit to some node B, node B doesn't necessarily have the ability to transmit to node A.
2) All nodes have loosely synchronized clock, and have the ability to define its location in order to perform neighbor authentication. Security at hardware level is not possible in the network considered. Further, each node has its private/public key pair, and has the ability to know the public keys of all other nodes.

### *C. Description of the Work:*

1) The process starts as the nodes are deployed in the network. The clusters are formed and in each clusters the randomly one Certification Agent each cluster is formed.
2) These agents are responsible for the authentication purpose. The node who wants to communicate initiate the process by generating its pass identifier and sending it to its cluster's CA.
3) The CA registers it after authentication and send it to other nodes present for the same purpose. The authentication and verification is done with this Pass identifier.
4) This process is repeated in the network when a new node wants to communicate with another node.
5) When the messages are sent by the source node they contain the same Pass Identifier.
6) In this way the nodes will be able to communicate securely and the network security is increased.

## IV. PSEUDO CODE

Generate Pass Identifier:
{
L<- Node's location (GPS)
Digest <- Cryptographic contents
Break the digest into four parts ($D_0 – D_3$)
Pass Identifier <- Concatenate (MAC, ($D_0$ XOR $D_1$ XOR $D_2$ XOR $D_3$ XOR L)

All rights reserved by *www.ijste.org*

Return Pass Identifier
}
After obtaining the Pass Identifier, security mechanism is performed as:-

1) The mobile node sends update message containing the Pass Identifier to the Certification Agent in the cluster.
2) The corresponding Certification Agent replies with the information.
3) After receiving the reply, the mobile node verifies the content and check if it is authorized to do so.
4) The certifying agent distributes this information about the node to other nodes in the network.
5) This information is checked with the message when it is sent across the network.
6) If a node receiving the packet gets the same Pass Identifier, then it performs the required action i.e. receiving, forwarding, broadcasting etc.
7) Otherwise, it ignores the message packets, which protects the network from any kind of damage.
8) As a result of this technique the network performs much securely as compared to the traditional one.

## V. SIMULATION RESULTS

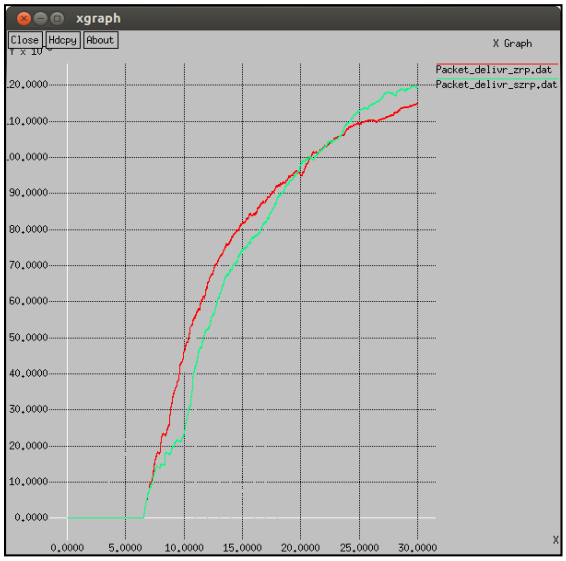

Fig. 1: Comparison of PDR

The graph comparison of PDR shows the comparison of the traditional approach with the new proposed secure ZRP. The new approach takes some time to built the complete setup in the network and for network configuration which results in the less value of PDR in the initial phase of network simulation. As the time passes the network recovers as a result of reduction in the computational load , at the end the new proposed algorithm is having higher values of PDR with respect to the traditional ZRP.

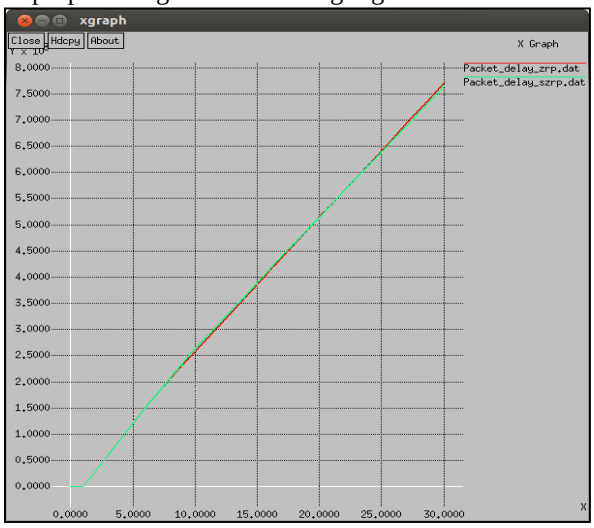

Fig. 2: Comparison of Overhead

All rights reserved by *www.ijste.org*

The overhead graph clearly shows the effect of the computational overhead which is involved in the security mechanism in the proposed scheme. For about 7 sec the two graph overlap each other , then the computational overhead of the proposed increases slightly and it remains higher than the traditional one for a time period from 7 Sec to 23 sec. Then it overlaps again, showing some reduction and this reduction continues in the further processing and as a result in the last the proposed scheme is having lesser overhead than the traditional one. This plots proves the point that initially the overhead is more than the traditional approach but as the network gains the maturity with time the overhead due to the computational steps reduces and resulting in lesser overhead than the traditional one.

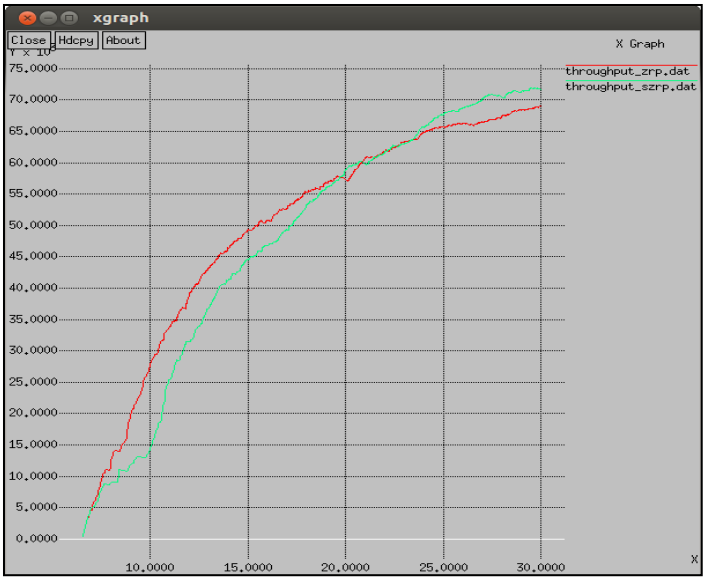


Fig. 3: Throughput Comparison

Throughput is the clear indicator of the performance of the network. It gives the information about the rate of data transfer in the network as , the plot for this is examined , the end results for the graph and the network shows that the throughput of the proposed scheme is more than that of the traditional approach.

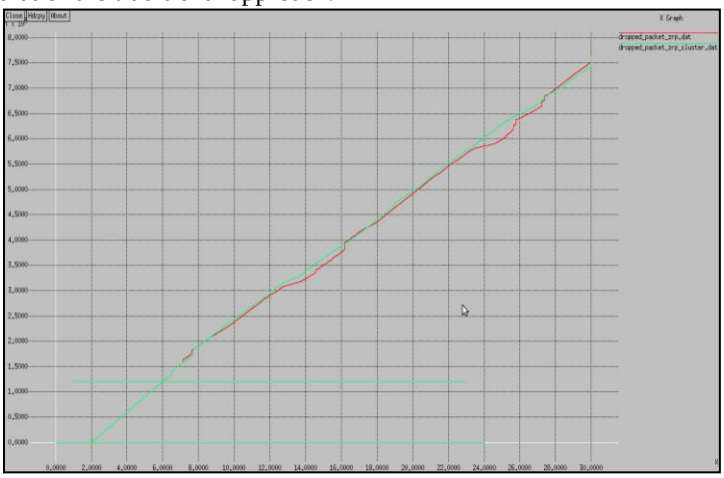

Fig. 4: Drop Packet Comparison of Two Approaches

Drop Packets are the packets which lack the delivery in the network due to some of the delays and inability of the network to handle the packets which are generated at an extent. Overall analysis of the graph shows that the packets dropped by the network in case of proposed scheme are lesser than the traditional approach.

## VI. CONCLUSION

In this paper, the ZRP in two different implementations is analyzed, one is the simple ZRP protocol where the normal functions as another application uses the secure ZRP protocol that consists with the help of the proposed security system. This scheme is proposed to improve the efficient and adaptable protocol network scenario so it can be more efficient in the performance than the single ZRP protocol. The implementation is done in the modification of the routing process which leads ultimately to a higher

All rights reserved by *www.ijste.org*

speed and higher packet loss rate and less packet loss. The results obtained are in coordination with the objective selected for this implementation.

## REFERENCES

[1] A.Anna lakshmi and Dr. K. R. Valluvan. "A Survey of Algorithms for Defending MANETs against the DDoS Attacks." International Journal of Advanced Research in Computer Science and Software Engineering, Volume9, Issue9, September 2012.
[2] Anil Kumar Sharma, Pankaj Singh Parihar. "An Effective DoS Prevention System to Analysis and Prediction of Network Traffic Using Support Vector Machine Learning." International Journal of Application or Innovation in Engineering & Management(IJAIEM), Volume 2, Issue 7, July 2013.
[3] Arunmozhi Annamalai and Venkataramani Yegnanarayanan. "Secured System against DDoS Attack in Mobile Adhoc Network." Weseas Transactions on Communications,Volume11, Issue 9, September 2012.
[4] Bansal, Meenakshi, Rachna Rajput, and Gaurav Gupta. "Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations." (1999).
[5] C. K. Nagpal, Chirag Kumar, Bharat Bhushan, Shailender Gupta, "A Study of Black Hole Attack on MANET Performance", I.J.Modern Education and Computer Science(2012),47-53.
[6] Chin, Kwan-Wu, et al. "Implementation experience with MANET routing protocols." Publish in ACM SIGCOMM Computer Communication Review 32.5 (2002): 49-59
[7] Fei Xing and Wenye Wang. "Understanding Dynamic Denial of Service Attacks in Mobile Ad Hoc Networks."2011
[8] Gorantala, Krishna. "Routing protocols in mobile ad-hoc Networks." A Master'thesis in computer science, pp-1-36 (2006)
[9] Guarnera, M., et al. "MANET: possible applications with PDA in wireless imaging environment." Personal, Indoor and Mobile Radio Communications, 2002. The 13th IEEE International Symposium on. Vol. 5. IEEE, 2002.
[10] Gurjinder Kaur, Yogesh Chaba and V.K. Jain. "Distributed Denial of Service Attacks in Mobile Adhoc Networks." World Academy of Science, Engineering and Technology 49 2011.
[11] http://www.ijmer.com/papers/Vol3_Issue2/BO32845848.pdf
[12] http://www.dauniv.ac.in/downloads/Mobilecomputing/MobileCompChap11L02MANETPropertiesandSpectrumRequir.pdf
[13] Jonny Karlsson, Laurence S. Dooley, Goran Pulkkis, "Routing Security in Mobile Ad-hoc Networks",Issues in Informing Science and Information Technology, Volume 9, 2012.
[14] K. Urmila Vidhya and M. Mohana Priya. "A Novel technique for defending routing attacks in OLSR Manet." 2010 IEEE International Conference on Computational Intelligence and Computing Research.
[15] Lee, Unghee, Scott F. Midkiff, and Jahng S. Park. "A proactive routing protocol for multi-channel wireless ad-hoc networks (DSDV-MC)." Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on. Vol. 2. IEEE, 2005
[16] Mahmood Salehi and Hamed Samavati. "Injection and Evaluation of New Attacks on Ad hoc Proactive Routing Algorithms." International Journal for Information Security Research (IJISR), Volume 2, Issue ½, March/June 2012.
[17] Mieso K. Denko. "Detection and Prevention of Denial of Service(DoS) Attacks in Mobile Ad Hoc Networks using Reputation-Based Incentive Scheme." Systemics, Cybernetics and Informatics, Volume 3, Number 4,2011.
[18] Mukesh Kumar & Naresh Kumar. "Detection and Prevention of DDoS attack in MANET's using disable IP broadcast Technique." International Journal of Application or Innovation in Engineering & Management (IJAIEM) , Volume 2, Issue7, July 2013.

All rights reserved by *www.ijste.org*